CrypTool

Modern open-source e-learning programs for cryptography and cryptanalysis

Professor Bernhard Esslinger, University of Siegen

April 23rd, 2013

FRISC-Winter School FINSE

UNIVERSITÄT SIEGEN

Agenda

1	Why we created CrypTool
2	Context and basics of cryptography
3	 Cryptography with the offline programs CT1, CT2 and JCT
4	CT websites: CTP (CT Portal), CTO (CrypTool Online), MTC3

Abbreviations used:

CT	CrypTool
CT1	CrypTool v1
CT2	CrypTool v2
JCT	JavaCrypTool

Sub Agenda

1	Why we created CrypTool
2	Context and basics of cryptography
3	Cryptography with the offline programs CT1, CT2 and JCT
4	CT websites: CTP (CT Portal), CTO (CrypTool Online), MTC3

What Happens with the Implementations of Research Results?

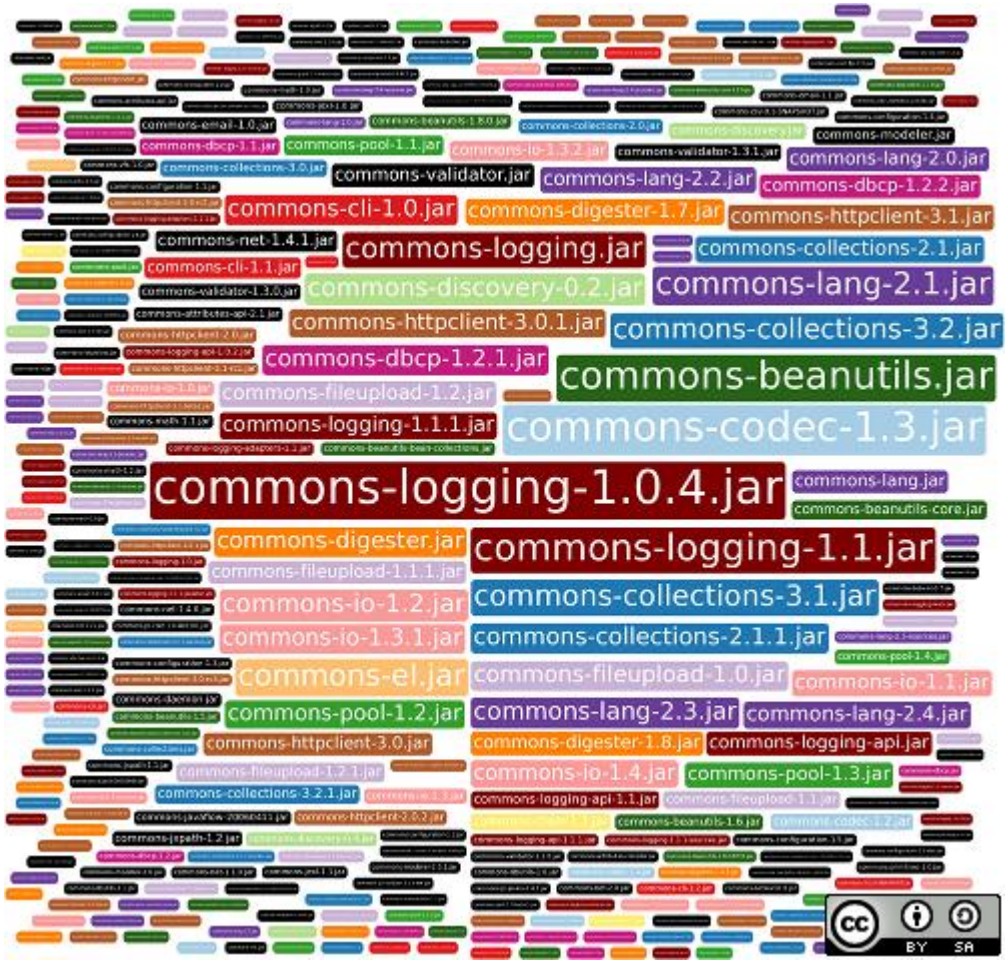
http://commons.wikimedia.org/wiki/File:Universit%C3%A4t_Bonn.jpg

http://commons.wikimedia.org/wiki/File:Bin.JPG

Framework for Results in Cryptography / Cryptology

http://commons.wikimedia.org/wiki/File:Simplified_VA_Zachman_Framework.jpg
http://commons.wikimedia.org/wiki/File:Architecture_framework.jpg

How to Set up an Open-Source Project – 99 % of them are Dead?



http://commons.wikimedia.org/wiki/File:Opensource.svg Logo of the Open Source Initiative
http://commons.wikimedia.org/wiki/File:Project_reuse_ranking_apache_commons_library.png

Successful OS Projects: Make Many People Benefit, Make Many People Contribute, Spread the Word, and Start Again.

Contributing Universities (contributing crypto plugins)

— Belgrad, Berlin, Bochum, Bonn, Brisbane,
Brno, Darmstadt, Dubai, Duisburg-Essen, Eindhoven,
Hagenberg, Jena, Karlsruhe, Kassel,
Klagenfurth, Koblenz, London, Madrid,
Mannheim, Osnabrück, San Jose, Siegen,
Thessaloniki, Utrecht, Warsaw, …

Contributing People

— 60 volunteers, both experts and beginners
from all over the world

— Keep the main contributors and the core team happy

High Responsiveness; Administrators to run the website securely and stable

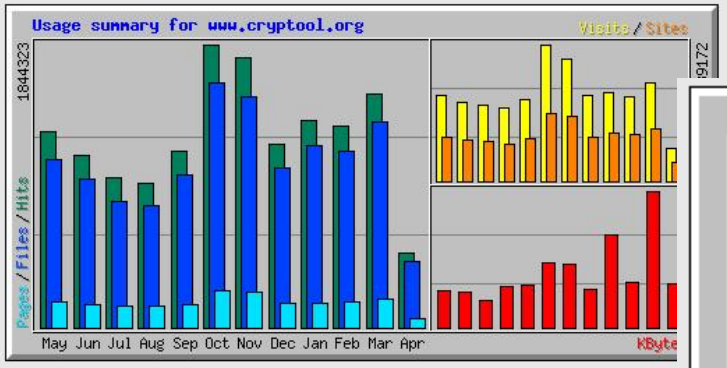
— We try to answer each mail within 2 days (we are getting circa 3 mails from users per day).

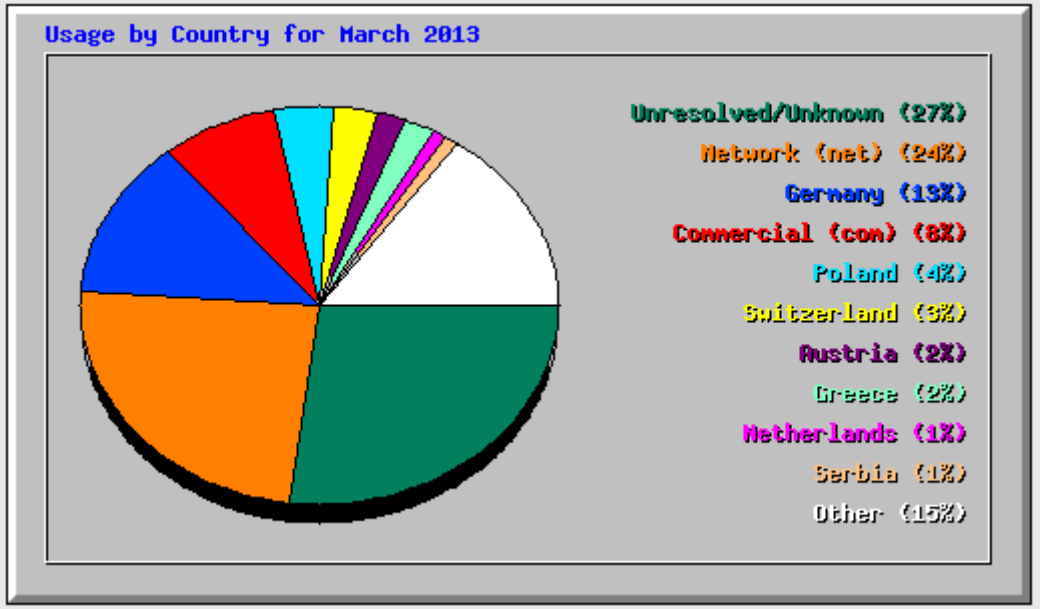
— Some effort is needed to keep Linux, PHP, Joomla and all other tools up-to-date.

What about the Users? It's More than just Website Analytics.

Usage Statistics for www.cryptool.org

Summary by Month
Generated 11-Apr-2013 04:20 CEST





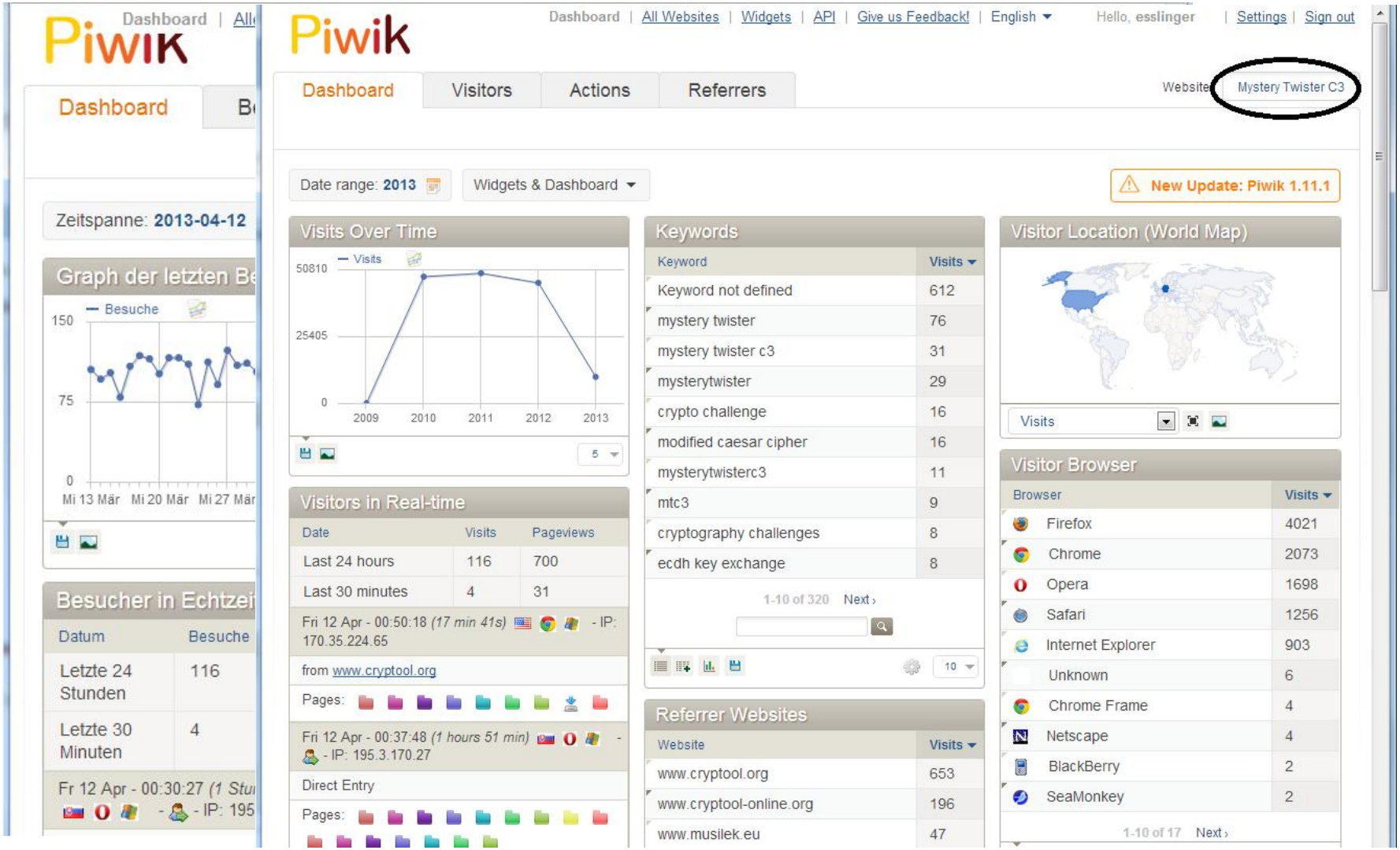
Summary by Month

Month	Daily Avg				Monthly Totals				
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files
Apr 2013	43978	38854	5517	849	5475	488303340	9346	60692	427401
Mar 2013	49016	43106	6024	913	15094	1527585913	28326	186766	1336293
Feb 2013	46878	41048	6088	863	13488	505718929	24186	170467	1149360
Jan 2013	43389	38319	5226	819	13776	1030152799	25393	162015	1187918
Dec 2012	38573	33599	5054	797	12789	434647404	24734	156701	1041577
Nov 2012	58693	50146	7808	1167	18599	703943790	35039	234240	1504408
Oct 2012	59494	51332	7864	1263	19208	723527900	39172	243788	1591319
Sep 2012	38456	33222	5010	780	12151	474482038	23415	150315	996674	1153687
Aug 2012	30271	25552	4530	675	10680	462133378	20950	140459	792127	938423
Jul 2012	31552	26452	4677	705	11460	308547557	21877	145013	820021	978140
Jun 2012	37516	32165	4934	755	11865	394995635	22650	148045	964972	1125485
May 2012	41073	35433	5460	795	12444	412363243	24654	169282	1098453	1273269
Totals						**7466401926**	**299742**	**1967783**	**12910523**	**14930868**

Generated by Webalizer Version 2.23

What about the Users? It's More than just Website Analytics.

MTC3 usage for one day and for the first circa 100 days in 2013



Target Users – Audience

The CrypTool project now exists since 15 years !

Audience

— Students

— Pupils

— Teachers

— Post Docs

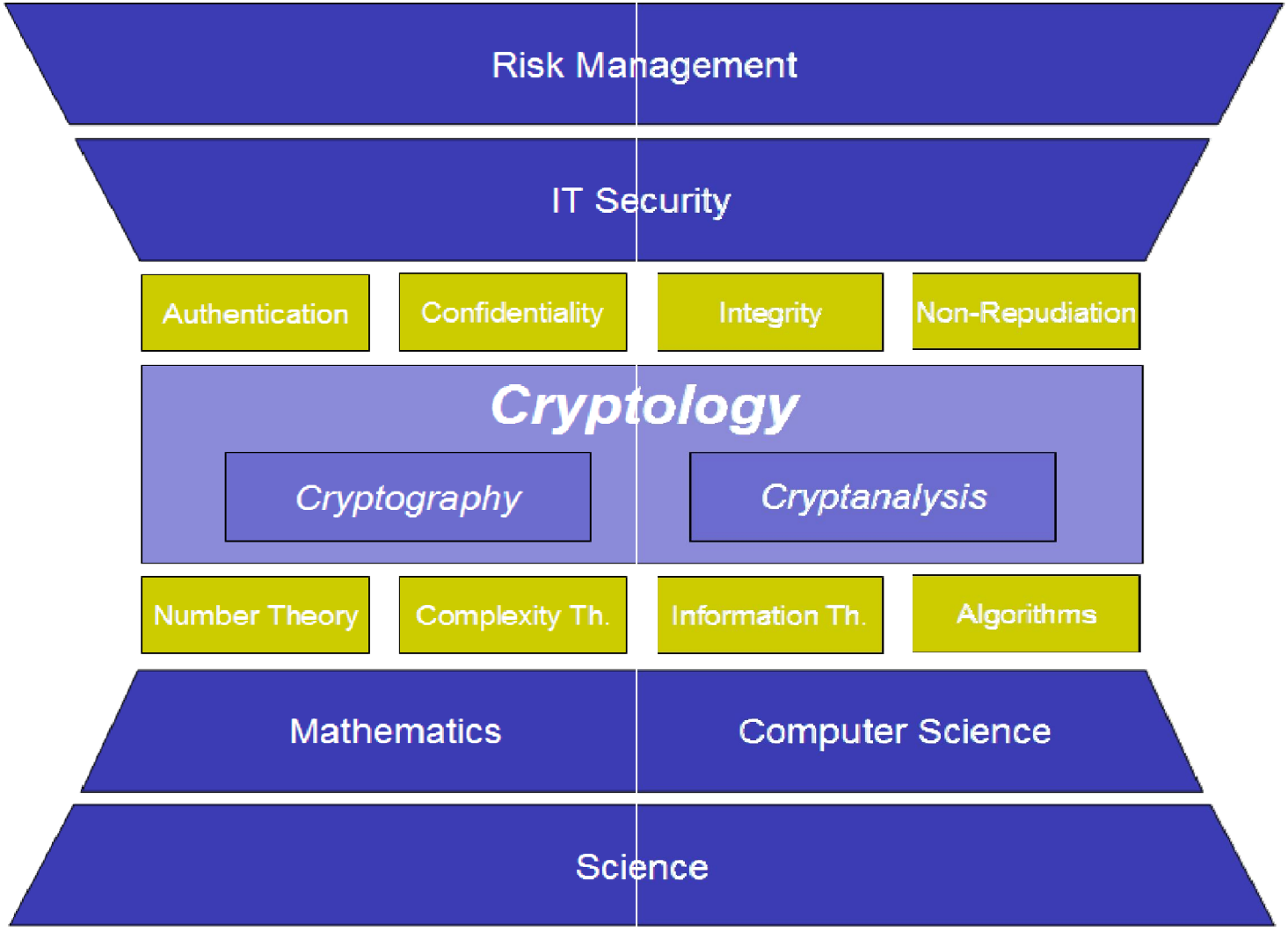
— Lecturers

Mission

— Raise the number of pupils and students to study a MINT subject, and

— Offer a modern e-learning tool to help them succeed when studying information security / cryptography

Context of Cryptography / Cryptology



Context of Cryptography / Cryptology

Content

I. Context and basics of cryptography

II. Cryptography with CT1, CT2 and JCT (offline programs)

III. CT websites

- CT Portal
- CTO (CrypTool Online)
- MTC3 (MysteryTwister C3) International cipher contest

Sub Agenda

1	Why we created CrypTool
2	Context and basics of cryptography
3	Cryptography with the offline programs CT1, CT2 and JCT
4	CT websites: CTP (CT Portal), CTO (CrypTool Online), MTC3

Relevance of Cryptography

Examples of applied cryptography

- Phone cards, cell phones, remote controls
- Cash machines, money transfer between banks
- Electronic cash, online banking, secure email
- Satellite TV, Pay TV
- Immobilizer systems in cars
- Digital Rights Management (DRM)

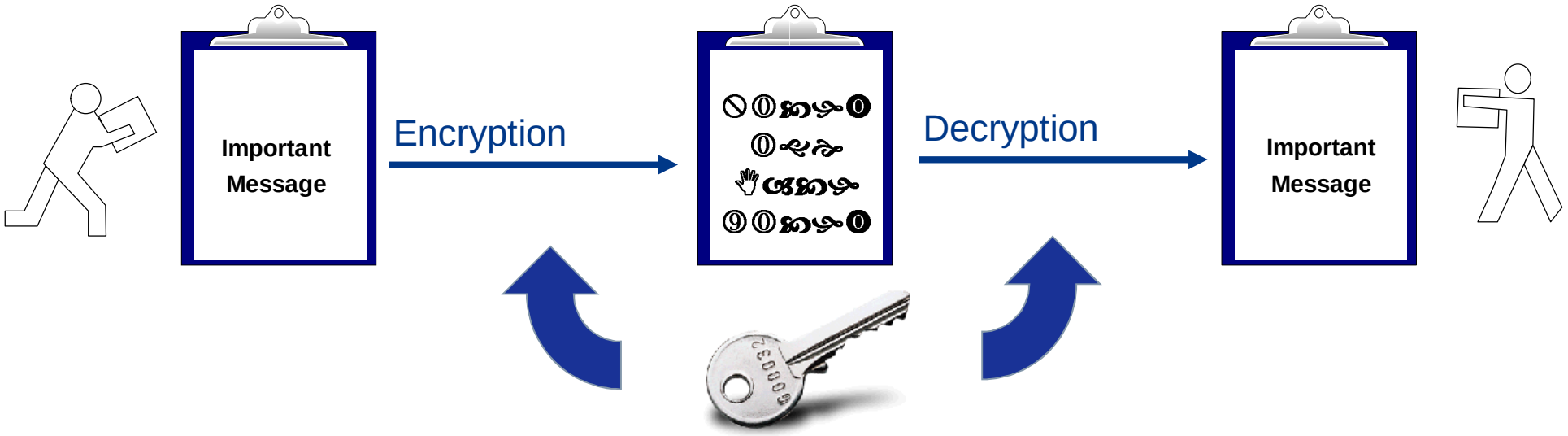
- Cryptography is no longer limited to agents, diplomats, and the military. Cryptography is a modern, mathematically characterized science.
- The breakthrough of cryptography followed the broadening usage of the Internet.
- For companies and governments it is important that systems are secure and that…

users (i.e., clients and employees) are aware of and understand IT security!

Symmetric Cryptography
Basics

Symmetric ciphers

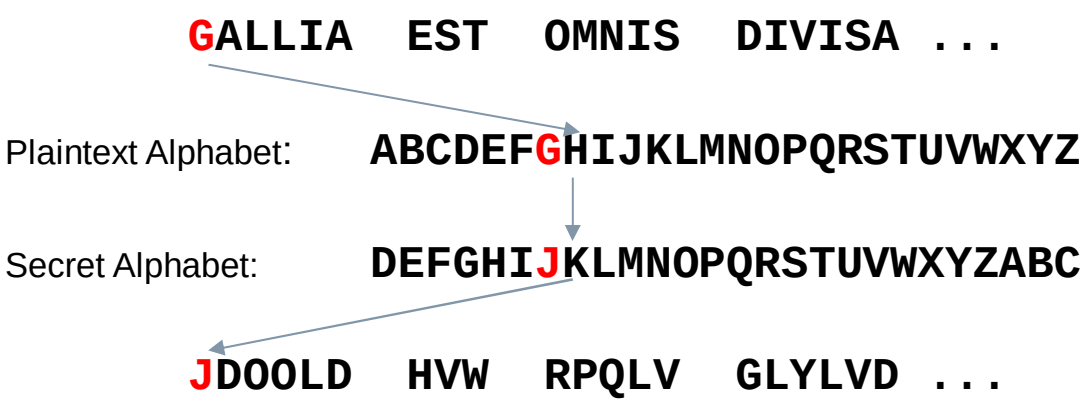
- Encryption and decryption by a shared key
- Sender encrypts using this key
- Recipient decrypts using the same key
- **Problem**: Key has to be transmitted securely

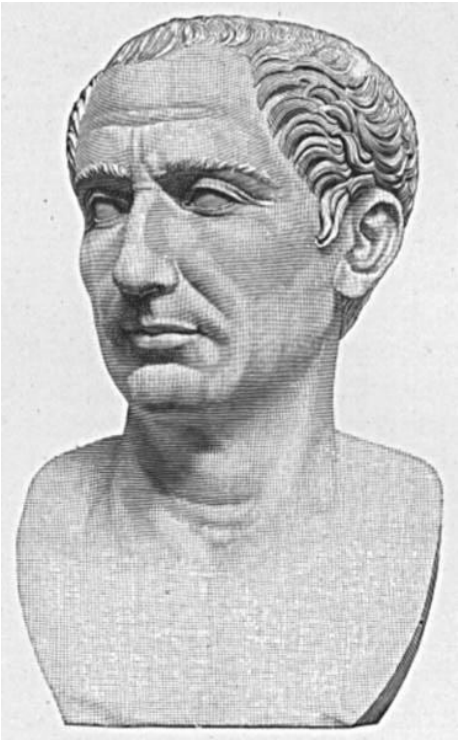


Examples for Symmetric Encryption (1)
Caesar cipher

— **Caesar cipher** (Julius Caesar, 100 - 44 AC)

— Simple substitution cipher





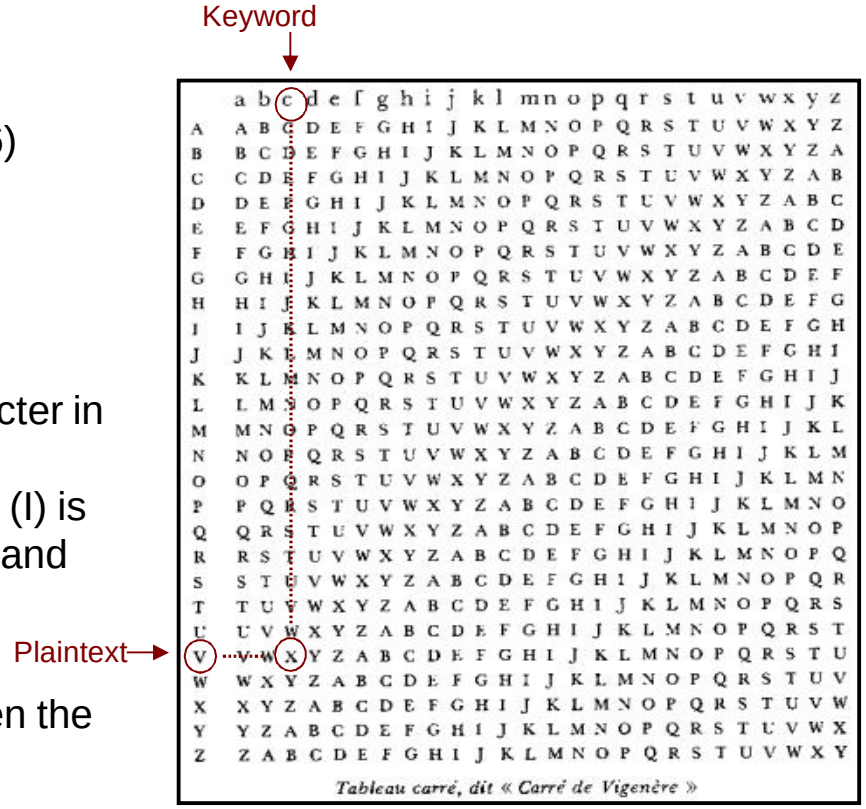
— Attack: Frequency analysis (typical characters allocation)

Example in CrypTool: ***www.cryptool.org***

Examples for Symmetric Encryption (2)

Vigenère cipher

- **Vigenère cipher** (Blaise de Vigenère, 1523-1596)
- Encryption with a keyword using a key table
- Keyword: **CHIFFRE**
- Encryption: **VIGENERE** becomes **XPOJSVVG**
- The plaintext character (V) is replaced by the character in the corresponding row and in the column of the first keyword character (c). The next plaintext character (I) is replaced by the character in the corresponding row and in the column of the next keyword character (h), and so on.
- If all characters of the keyword have been used, then the next keyword character is the first key character.



- **Attack** (via Kasiski test; other tests also exist): Plaintext combinations with an identical cipher text combination can occur. The distance of these patterns can be used to determine the length of the keyword. An additional frequency analysis can then be used to determine the key.

Examples for Symmetric Encryption (3)
Encryption using the Enigma

Enigma machine (Arthur Scherbius, 1878-1929)

- More than 200,000 machines were used in WWII.
- The rotating cylinders encrypt every character of the text with a new permutation.
- The Polish Cipher Bureau broke the pre-war Enigma prototype as early as 1932.
- Based on this work, the later Enigma was broken only with massive effort. About 7000 cryptographers in the UK used decryption machines, captured Enigma prototypes, and intercepted daily status reports (such as weather reports).
- **Consequences of the successful cryptanalysis**
  "The successful cryptanalysis of the Enigma cipher was a strategic advantage that played a significant role in winning the war. Some historians assert that breaking the Enigma code shortened the war by several months or maybe by a whole year."

  translated from http://de.wikipedia.org/wiki/Enigma_%28Maschine%29 - March 6, 2006

DES, 3DES and AES

Modern algorithms for symmetric encryption

- **DES** – Data Encryption Standard
  - Published as a standard for all American federal agencies in January 1977
  - 56 bits key length
  - **Problem**: Modern hardware offers fast brute-force attacks
- **3DES** – Improved DES
  - Encryption with 3 DES keys (typically in EDE mode*)
  - 112 bits effective key length
  - **Problem**: Encryption using 3 keys is ineffective
- **AES** – Advanced Encryption Standard (October 2000 by Joan Daemen, Vincent Rijmen)
  - Result of a tendering by NIST (National Institute of Standards and Technology)
  - Key lengths of 128, 192, 256 bits
  - **Usage of AES** – amongst others in protocols like SSL, SSH, IPsec, hard drive encryption E+, Wireless LAN 802.11i, contents auf Blackberries etc.

One-Time Pad (OTP)

Provably secure symmetric encryption

- **Example:** We assume that a one-time pad is used to encode the word "CRYPTOOL“.
- If an attacker tries to brute force the content of the pad, the message will decrypt into **every possible combination** of 8 characters.

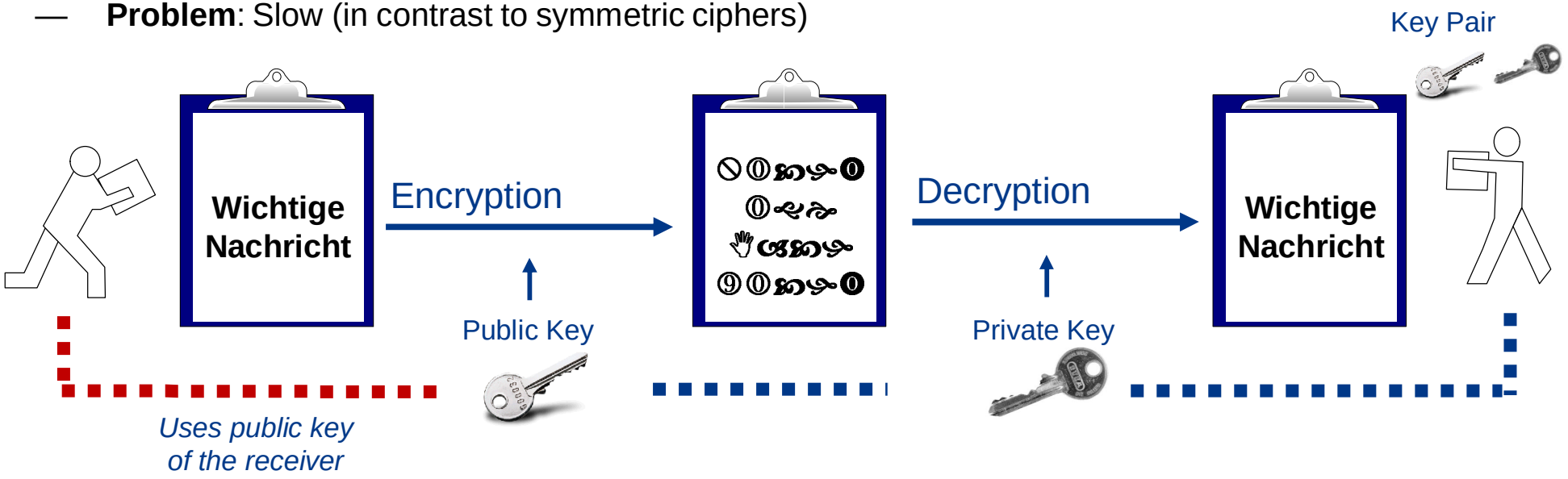
CIPHER-TEXT (hex)	KEY (hex)	CLEAR-TEXT (hex)	CLEAR-TEXT (txt)
11 1B 1E 18	52 49 47 48	43 52 59 50	CRYPTOOL
11 1B 1E 18 00 04 0A 15	41 5A 50 57 52 45 47 54	50 41 4E 4F 52 41 4D 41	PANORAMA
11 1B 1E 18 00 04 0A 15	54 57 5B 48 48 45 44 41	45 4C 45 50 48 41 4E 54	ELEPHANT
11 1B 1E 18 00 04 0A 15	50 55 5B 55 4F 4A 4F 46	41 4E 45 4D 4F 4E 45 53	ANEMONES
11 1B 1E 18 00 04 0A 15	52 53 5F 55 50 4D 45 5B	43 48 41 4D 50 49 4F 4E	CHAMPION
...	...	...	...

- Since the pad is truly random there are no statistical methods that the attacker can hope to use to infer which combination is correct.

Asymmetric Cryptography
Basics

Asymmetric ciphers

- **Solution** for the key distribution problem
- Each user has a public and a private key
- Sender encrypts with recipient's public key
- Recipient decrypts with his own private key
- **Problem**: Slow (in contrast to symmetric ciphers)



Hybrid Encryption and Certificates
Basics

– **Hybrid encryption** – **combination of asymmetric and symmetric encryption**

1. Generation of a random symmetric key (session key)
2. Session key is transferred – protected by asymmetric key
3. Message is transferred – protected by session key

– Problem**: Man-in-the-middle attacks –**
does the public key of the recipient really belong to the recipient?

– Solution: **Digital certificates –** a **central instance** (e.g., GlobalSign, Telesec, VeriSign, Thawte, company PKIs), trusted by all users, **ensures the authenticity** of the certificate and the associated public key (similar to a passport issued by a national government).

– Hybrid encryption based on digital **certificates is the foundation for all secured electronic communication**

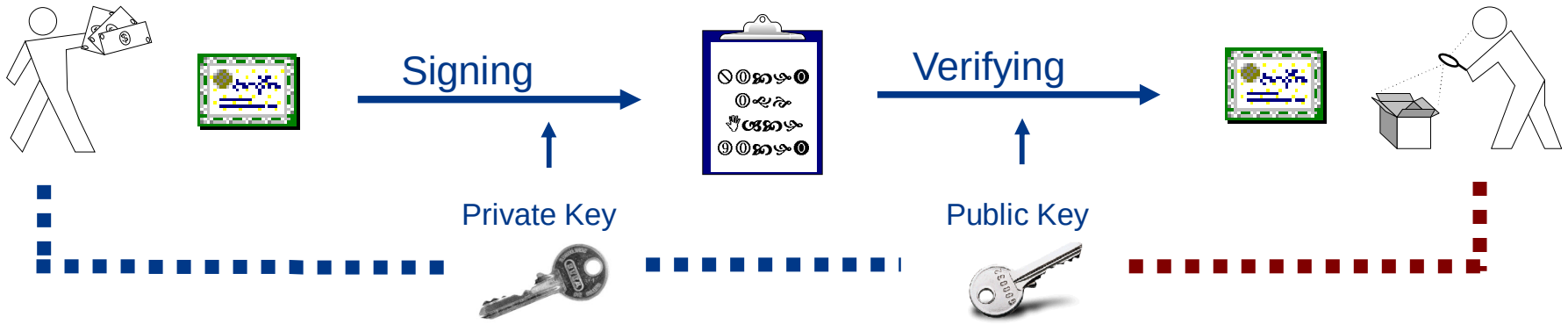
– Internet shopping and online banking

– Secure email

Digital Signature

Authenticity through the digital signature by the issuer

- **Problem: How to ensure the authenticity of a certificate?**
- **Solution: Issuer signs the certificate!**
- Digital signature proceeds analogously to asymmetric ciphers (but using the keys inversely)
  1. The certificate (or the hash value of the certificate to be exact) is signed with the private key of the issuer.
  2. The signed certificate can be verified by any user with the issuers public key. A successful verification means the certificate is authentic as only the issuer is able to sign the certificate with its private key.



* The hash value of a document is a distinct check number of its content. Changes in the content will cause a different hash value. Hashes aim to protect the integrity.

Conclusion: What is Cryptography Offering?

Security goals are reached by cryptography

- Security goals of digital communication
  - **Confidentiality**
  - **Authentication**
  - **Integrity**
  - **Non-Repudiation**
- By using cryptography these goals can be reached!
  - Confidentiality:
    → via **symmetric, asymmetric und hybrid encryption**
  - Authentication, integrity and non-repudiation:
    → via certificates and **digital signatures**
- Cryptography is the foundation, to ensure **trust** in electronic communications.

Hard Drive Encryption

— Laptop hard drives encrypted e.g. with Microsoft BitLocker - TPM (Win7)

Windows 7

— **AES 128 / 256 bits – *Secure?*** *Basically yes, but…*

— **Problem**: Key is derived from password

— **Dictionary attack**: Users often choose weak passwords

— 256 Bit Key: 2^256 ≈ **1,16e+77 possible combinations**

— 26 characters in the alphabet, 52 including upper/lower case, 62 including numbers

TPM supports additional security

— 20 digit password: 62^20 ≈ **7,04e+35**

— 43 digit password: 62^43 ≈ **1,18e+77**
and: Uniformly distributed !

X3jpq83MeO2dKqypaq9w2Erm7wp0yXuvQd3r7gTv2S

Sub Agenda

1	Why we created CrypTool
2	Context and basics of cryptography
3	 Cryptography with the offline programs CT1, CT2 and JCT
4	CT websites: CTP (CT Portal), CTO (CrypTool Online), MTC3

Overview of CrypTool: Three Offline Programs plus Websites

CRYPTOOL version 1.4.31, http://www.cryptool.org

CRYPTOOL 2 http://www.cryptool.org/de/ct2-dokumentation-de

JCrypTool The cryptography e-learning platform. https://github.com/jcryptool/

CRYPTOOL-ONLINE http://www.cryptool-online.org

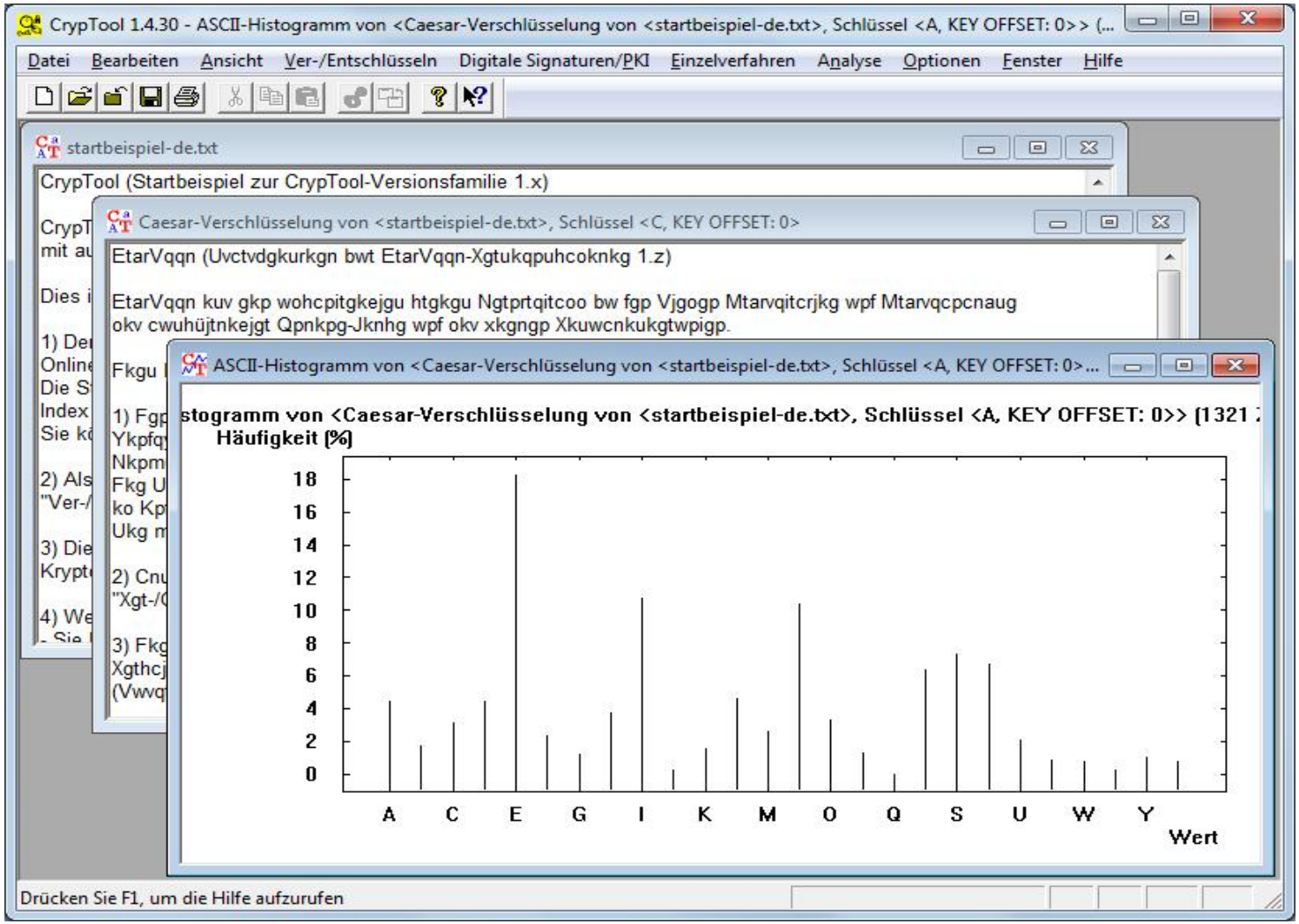
MysteryTwister C3 THE CRYPTO CHALLENGE CONTEST http://www.mysterytwisterc3.org/

CT1
www.cryptool.org/en

- CrypTool 1 [1.4.30 (released); 1.4.31 (stable)]
  - C++ under VS 2010, for Win32
  - Runs under Windows Vista, 7 and 8
  - Available in English, German, Spanish, Polish, Serbian and (soon) in Greek.

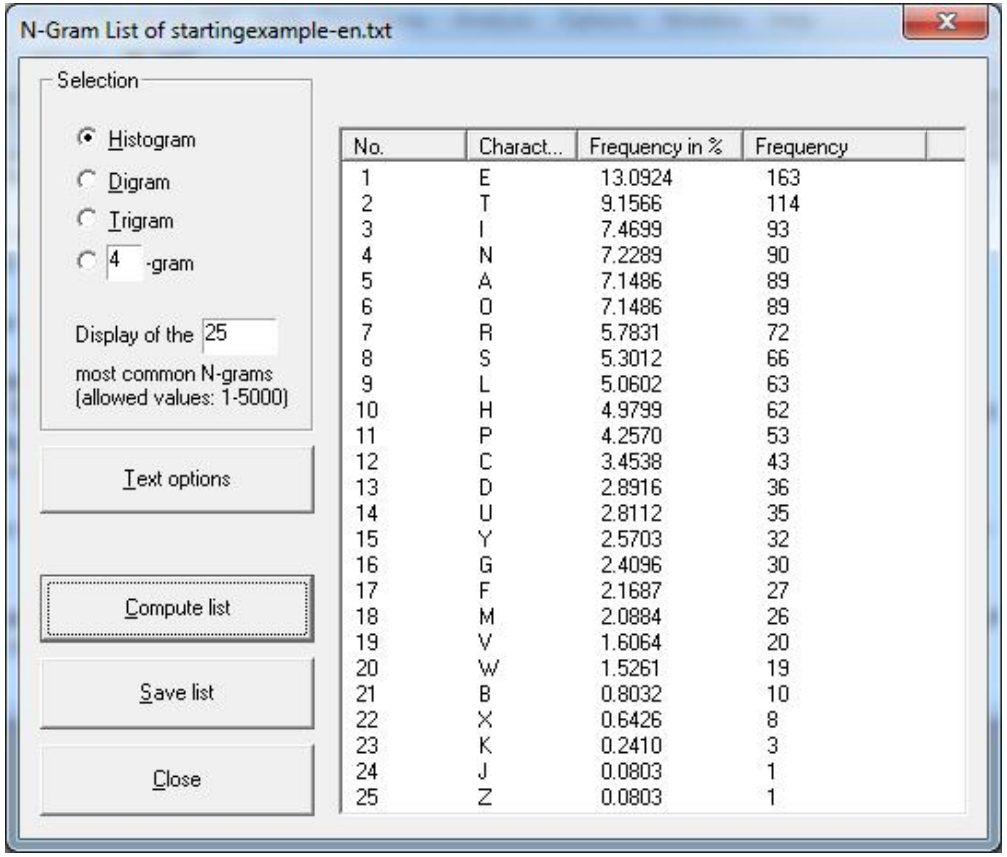
CT1

Example of a classic symmetric encryption (Caesar) and its analysis in CT1

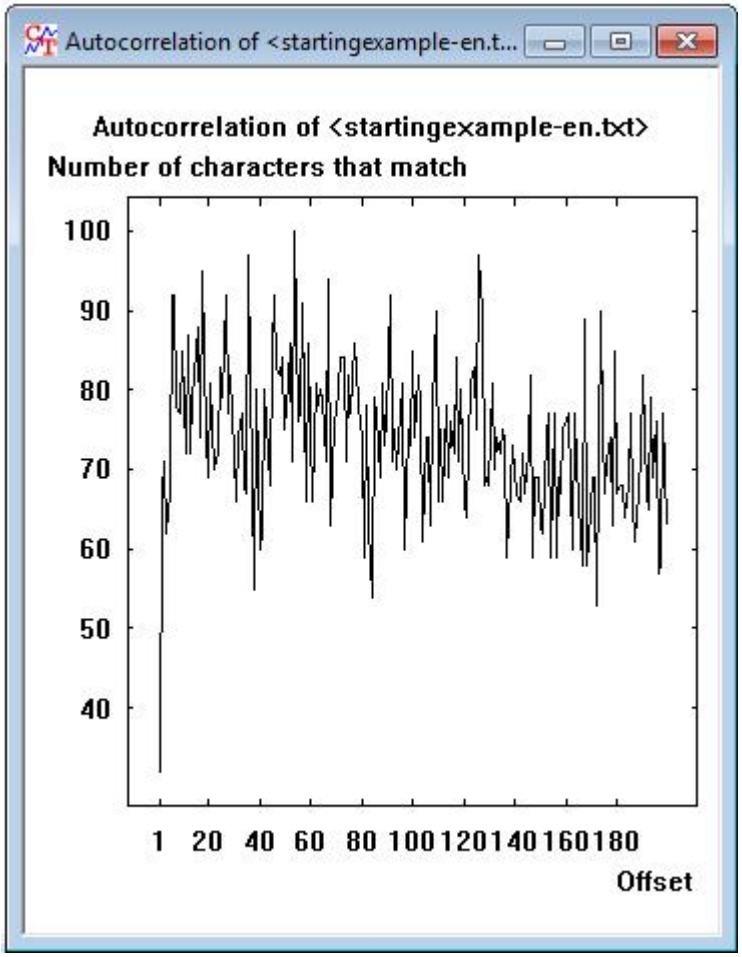


CT1

Analysis tools

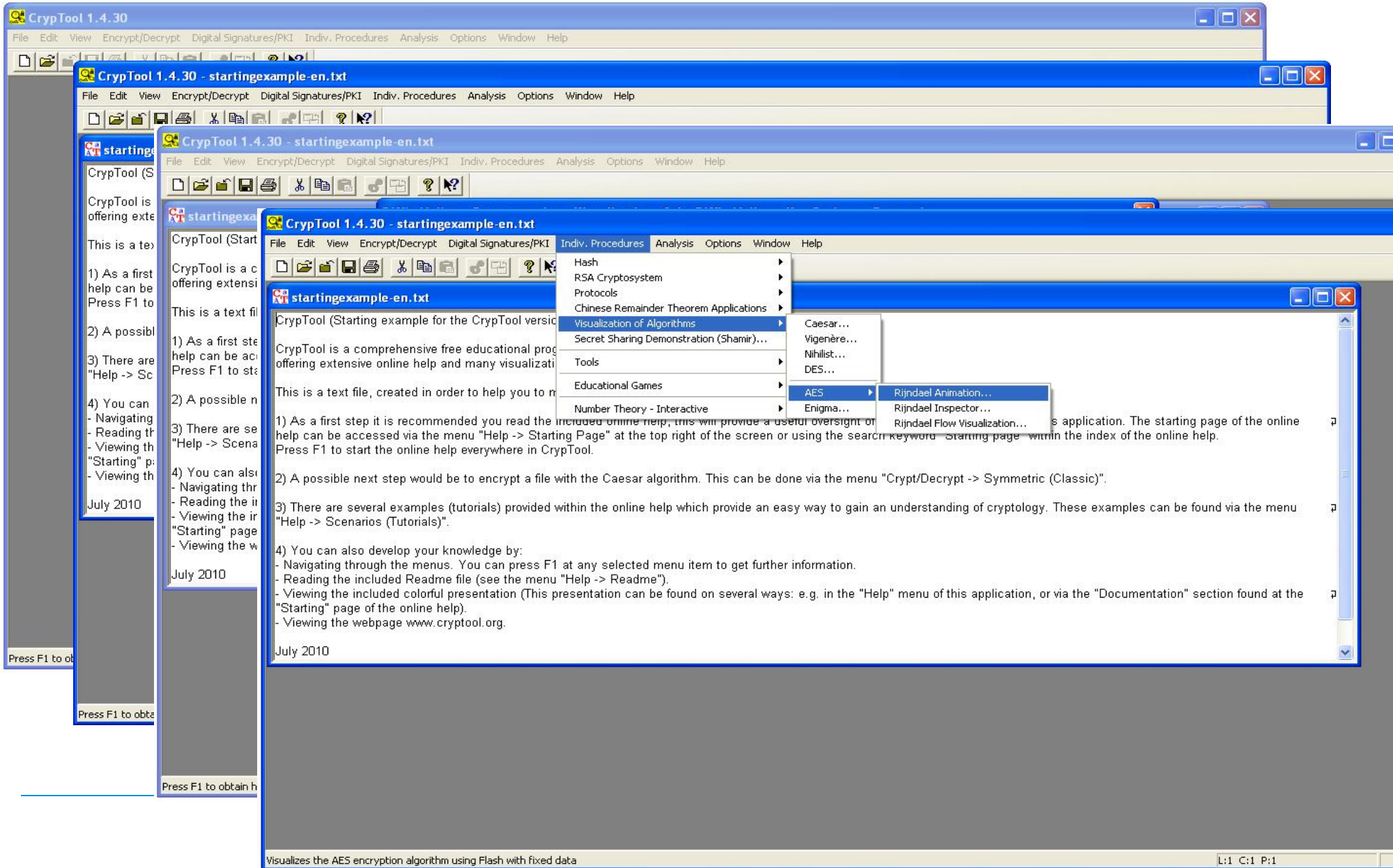


No.	Charact...	Frequency in %	Frequency
1	E	13.0924	163
2	T	9.1566	114
3	I	7.4699	93
4	N	7.2289	90
5	A	7.1486	89
6	O	7.1486	89
7	R	5.7831	72
8	S	5.3012	66
9	L	5.0602	63
10	H	4.9799	62
11	P	4.2570	53
12	C	3.4538	43
13	D	2.8916	36
14	U	2.8112	35
15	Y	2.5703	32
16	G	2.4096	30
17	F	2.1687	27
18	M	2.0884	26
19	V	1.6064	20
20	W	1.5261	19
21	B	0.8032	10
22	X	0.6426	8
23	K	0.2410	3
24	J	0.0803	1
25	Z	0.0803	1



* The screenshots here show results based on computing only upper case characters, setting are available in “Text options”.

CT1


CrypTool 1.4.30
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
CrypTool 1.4.30 - startingexample-en.txt
Hash
RSA Cryptosystem
Protocols
Chinese Remainder Theorem Applications
Visualization of Algorithms
Secret Sharing Demonstration (Shamir)...
Tools
Educational Games
Number Theory - Interactive
Caesar...
Vigenère...
Nihilist...
DES...
AES
Enigma...
Rijndael Animation...
Rijndael Inspector...
Rijndael Flow Visualization...
startingexample-en.txt
CrypTool (Starting example for the CrypTool versic
CrypTool is a comprehensive free educational prog
offering extensive online help and many visualizati
This is a text file, created in order to help you to n
1) As a first step it is recommended you read the included online help, this will provide a useful oversight of s application. The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the screen or using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CrypTool.
2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".
3) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".
4) You can also develop your knowledge by:
- Navigating through the menus. You can press F1 at any selected menu item to get further information.
- Reading the included Readme file (see the menu "Help -> Readme").
- Viewing the included colorful presentation (This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help).
- Viewing the webpage www.cryptool.org.
July 2010
Visualizes the AES encryption algorithm using Flash with fixed data
L:1 C:1 P:1

CT1 Features (1)

Cryptography

Classic cryptography

- Caesar (incl. ROT-13)
- Monoalphabetic substitution (incl. Atbash)
- Vigenère
- Hill
- Homophone substitution
- Playfair
- ADFGVX
- Byte addition
- XOR / Vernam / OTP
- Solitaire
- Permutation / Transposition
  (rail fence, skytale, double column transposition, …)

Several options to easily comprehend cryptography samples from literature

- Selectable alphabet
- Handling of special characters controllable

Cryptanalysis

Attack on classical methods

- Ciphertext-only
  - Caesar
  - Vigenère (according to Friedman + Schroedel)
  - Byte Addition
  - XOR
  - Substitution
  - Playfair
- Known plaintext
  - Hill
  - Single-column permutation/transposition
- Manual (program supported)
  - Monoalphabetic substitution
  - Playfair, ADFGVX, Solitaire

Supported analysis methods

- Entropy, floating frequency
- Histogram, n-gram analysis
- Autocorrelation
- Periodicity
- Random analysis

CT1 Features (2)

Cryptography

Modern symmetric encryption

- IDEA, RC2, RC4, RC6, DES, 3DES, DESX
- AES candidates of the last selection round (Serpent, Twofish, etc.)
- AES (=Rijndael)
- DESL, DESXL

Asymmetric encryption

- RSA with X.509 certificates
- RSA demonstration
  - For improved understanding of examples from literature
  - Alphabet and block length selectable

Hybrid encryption (RSA + AES)

- Visualized as an interactive data flow program

Cryptanalysis

Brute-force attack on symmetric algorithms

- For all algorithms
- Assumptions:
  - Entropy of plaintext is small,
  - Key is partially known, or
  - Plaintext alphabet is known

Attack on RSA encryption

- Factorization of RSA modulus*
- Lattice-based attacks

Attack on hybrid encryption

- Attack on RSA or
- Attack on AES (side-channel attack)

CT1 Features (3)

Cryptography

Digital signature

- RSA with X.509 certificates
  - Signature visualized as interactive data-flow-diagram
- DSA with X.509 certificates
- Elliptic Curve DSA, Nyberg-Rueppel

Hash functions

- MD2, MD4, MD5
- SHA, SHA-1, SHA-2, RIPEMD-160

Random generators

- Secude
- x^2 mod n
- Linear congruence generator (LCG)
- Inverse congruence generator (ICG)

Cryptanalysis

Attack on RSA signature

- Factorization of the RSA module
- Feasible up to 250 bits or 75 decimal digits (on standard desktop PCs)

Attack on hash functions / digital signature

- Generate hash collisions for ASCII based text (birthday paradox) (with 40 bits it takes approximately five minutes to find a collision for any hash function)

Analysis of random data

- FIPS-PUB-140-1 test battery
- Periodicity, Vitányi, entropy
- Floating frequency, histogram
- n-gram analysis, autocorrelation
- ZIP compression test

CT1 Features (4)

Visualization / Demos

- Caesar, Vigenère, Nihilist, DES (all with ANIMAL)
- Enigma (Flash)
- Rijndael/AES (two versions with Flash, and one with Java)
- Hybrid encryption and decryption (AES-RSA and AES-ECC)
- Generation and verification of digital signatures
- Diffie-Hellman key exchange
- Secret sharing with Chinese Remainder Theorem (CRT) and threshold scheme according Shamir
- Challenge-response method (network authentication)
- Side-channel attack
- Secure email with the S/MIME protocol (with Java and Flash)
- Graphical 3D presentation of (random) data streams
- Sensitivity of hash functions regarding plaintext modifications
- Number theory and RSA cryptosystem (with Authorware)

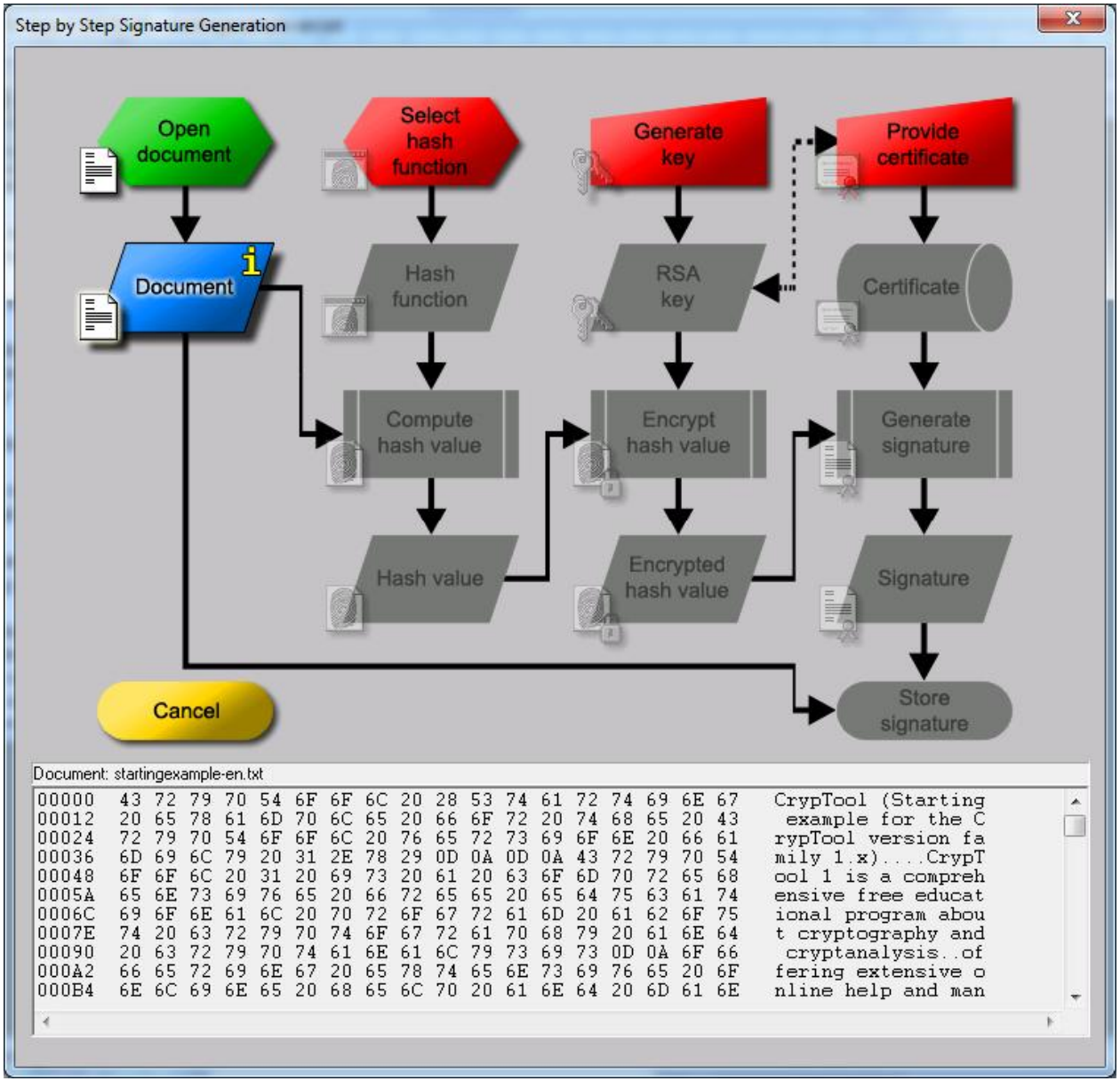
CT1 Features (5)

Additional functions

- Various functions for RSA and prime numbers
- Homophone and permutation encryption (double column transposition)
- PKCS #12 import and export for PSEs (Personal Security Environment)
- Hash generation of large files (without loading them)
- Flexible brute-force attacks on any modern symmetric algorithm
- Generic brute-force attacks on any hash function
- ECC demonstration (as Java application)
- Password Quality Meter (PQM) and password entropy
- Manifold text options for the classic ciphers
- Encoding (base64 / uu-encode)
- And plenty more…

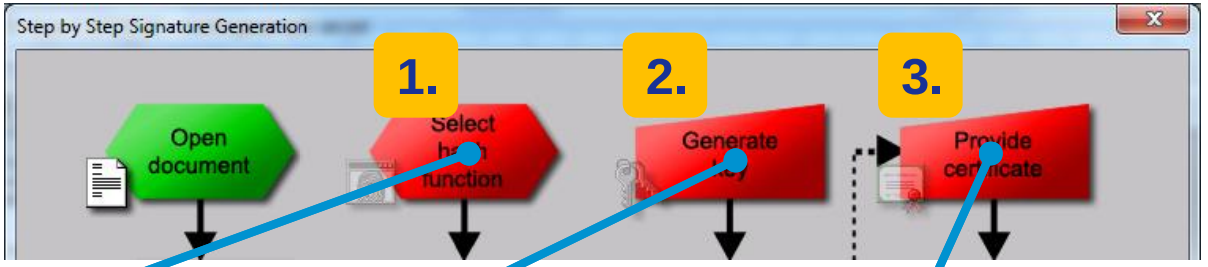
Demo

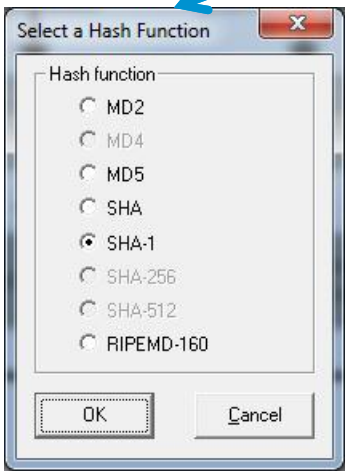
CT1

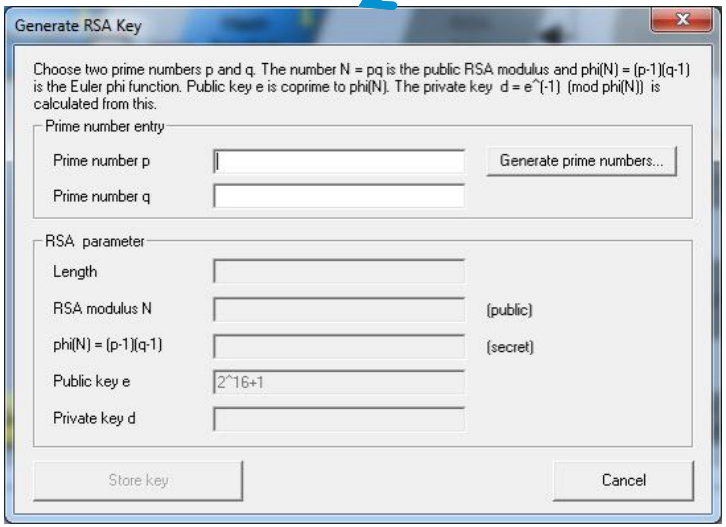

Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Document
Hash function
RSA key
Certificate
Compute hash value
Encrypt hash value
Generate signature
Hash value
Encrypted hash value
Signature
Cancel
Store signature
Document: startingexample-en.txt
00000 43 72 79 70 54 6F 6F 6C 20 28 53 74 61 72 74 69 6E 67 CrypTool (Starting
00012 20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43 example for the C
00024 72 79 70 54 6F 6F 6C 20 76 65 72 73 69 6F 6E 20 66 61 rypTool version fa
00036 6D 69 6C 79 20 31 2E 78 29 0D 0A 0D 0A 43 72 79 70 54 mily 1.x)....CrypT
00048 6F 6F 6C 20 31 20 69 73 20 61 20 63 6F 6D 70 72 65 68 ool 1 is a compreh
0005A 65 6E 73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 ensive free educat
0006C 69 6F 6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 ional program abou
0007E 74 20 63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 t cryptography and
00090 20 63 72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 cryptanalysis..of
000A2 66 65 72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F fering extensive o
000B4 6E 6C 69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E nline help and man

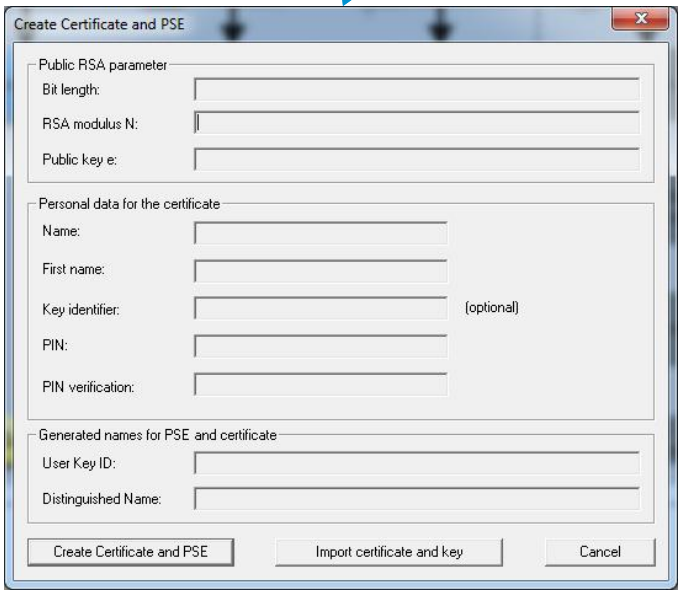
CT1

Reuse of components





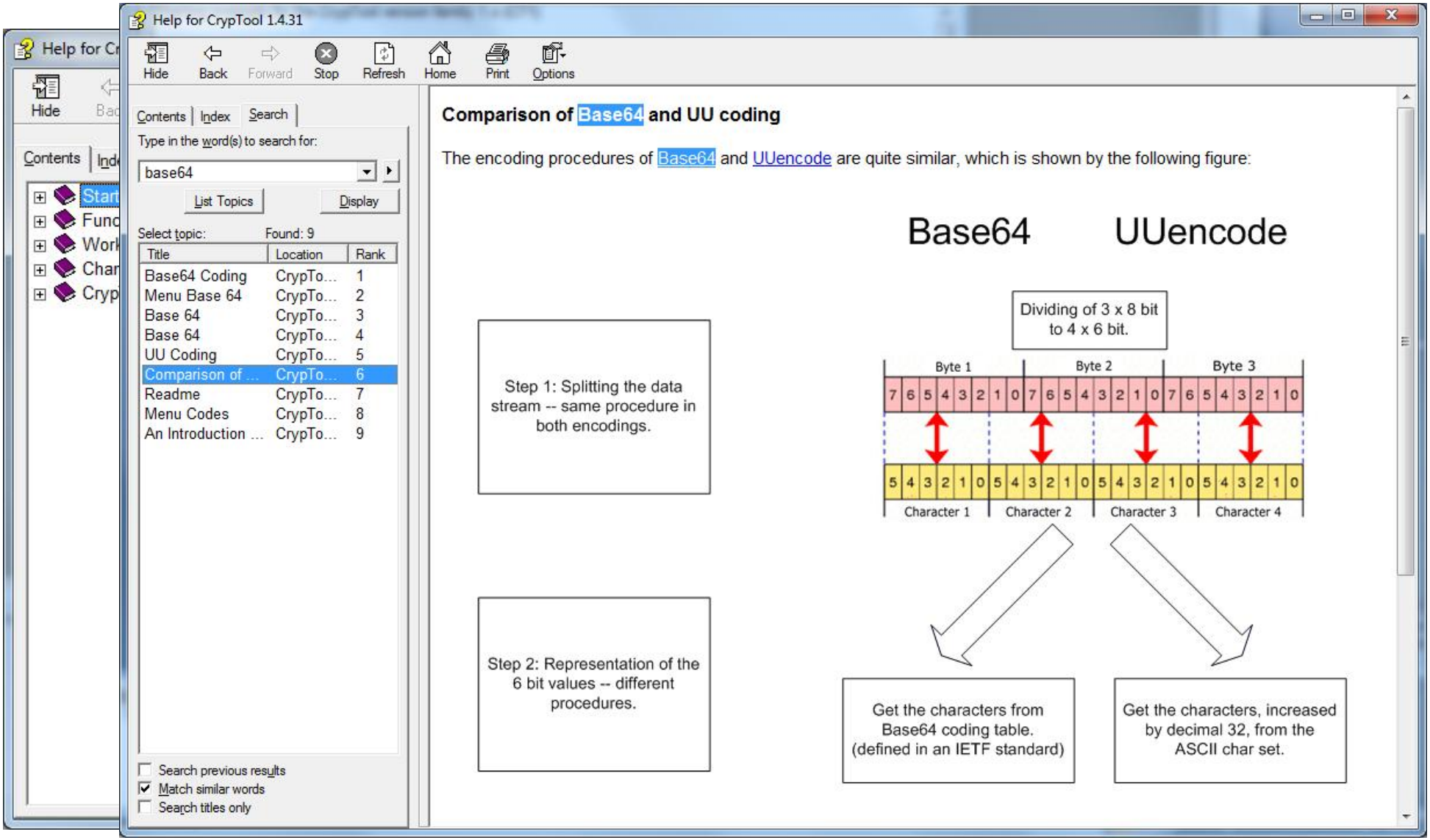




CT1 Menu Tree

- **File**
  - New
  - Open...
  - Close
  - Save
  - Save as...
  - Document Properties...
  - Print...
  - Print Setup...
  - Recent Files
  - Exit
- **Edit**
  - Undo
  - Redo
  - Cut
  - Copy
  - Paste
  - Delete
  - Find/Replace...
  - Find Next
  - Select All
  - Show Key...
  - Parent Window
- **View**
  - Toolbar
  - Status Bar
  - Show as Text
  - Show as HexDump
  - Bar Chart
  - Alphabet
  - End of Line
  - Line Wrap
  - Whitespace
  - Font
    - Arial 8
    - Arial 10
    - Arial 12
    - Arial 14
    - Arial 16
    - Courier 8
    - Courier 10
    - Courier 12
    - Courier 14
    - Courier 16
  - Format Text Document...
  - Show Box (cube's borderlines)
- **Encrypt/Decrypt**
  - Symmetric (classic)
    - Caesar / Rot-13...
    - Vigenère...
    - Hill...
    - Substitution / Atbash...
    - Playfair...
    - ADFGVX...
    - Byte Addition...
    - XOR...
    - Vernam / OTP...
    - Homophone...
    - Permutation / Transposition...
    - Solitaire...
    - Scytale / Rail Fence...
  - Symmetric (modern)
    - IDEA...
    - RC2...
    - RC4...
    - DES (ECB)...
    - DES (CBC)...
    - Triple DES (ECB)...
    - Triple DES (CBC)...
    - Rijndael (AES)...
    - Further Algorithms
      - MARS...
      - RC6...
      - Serpent...
      - Twofish...
      - DESX...
      - DESL...
      - DESXL...
    - AES (self extracting)...
  - Asymmetric
    - RSA Encryption...
    - RSA Decryption...
    - RSA Demonstration...
  - Hybrid
    - RSA-AES Encryption...
    - RSA-AES Decryption...
    - ECC-AES Encryption...
    - ECC-AES Decryption...
- **Digital Signatures/PKI**
  - PKI
    - Generate/Import Keys...
    - Display/Export Keys...
  - Sign Document...
  - Verify Signature...
  - Extract Signature
  - Signature Demonstration (Signature Generation)...
- **Indiv. Procedures**
  - Hash
    - MD2
    - MD4
    - MD5
    - SHA
    - SHA-1
    - SHA-256
    - SHA-512
    - RIPEMD-160
    - Hash Value of a File...
    - Hash Demonstration...
    - Key Generation from Password (PKCS #5)...
    - Generation of HMACs...
  - RSA Cryptosystem
    - Prime Number Test...
    - Generate Prime Numbers...
    - Factorization of a Number...
    - RSA Demonstration...
    - Signature Demonstration (Signature Generation)...
    - Lattice Based Attacks on RSA
      - Factoring with a Hint...
      - Attack on Stereotyped Messages...
      - Attack on Small Secret Keys...
  - Protocols
    - Diffie-Hellman Demonstration...
    - Network Authentication...
    - Secure E-Mail with S/MIME...
  - Chinese Remainder Theorem Applications
    - Astronomy and Planetary Motion...
    - Modular Foreward and Backward Transformation...
    - Secret Sharing by CRT...
  - Visualization of Algorithms
    - Caesar...
    - Vigenère...
    - Nihilist...
    - DES...
    - AES
      - Rijndael Animation...
      - Rijndael Inspector...
      - Rijndael Flow Visualization...
    - Enigma...
  - Secret Sharing Demonstration (Shamir)...
  - Tools
    - Codes
      - Base64 Encode/Decode
        - Base64 Encode
        - Base64 Decode
      - UU Encode/Decode
        - UU Encode
        - UU Decode
      - Decode ASN.1 Code of a Document
    - Compress
      - Zip
      - UnZip
    - Generate Random Numbers...
    - Password Quality Meter...
    - Password Entropy...
  - Educational Games
    - Number Shark
  - Number Theory - Interactive
    - Learning Tool for Number Theory...
    - Point Addition on Elliptic Curves...
    - Compute Mersenne Numbers...
- **Analysis**
  - Tools for Analysis
    - Entropy
    - Floating Frequency
    - Histogram
    - N-Gram...
    - Autocorrelation
    - Periodicity
  - Symmetric Encryption (classic)
    - Ciphertext-Only
      - Caesar
      - Vigenère
      - Vigenère (Analysis according to Schroedel)...
      - ADFGVX...
      - Substitution...
      - Solitaire...
      - Byte Addition
      - XOR / Vernam
    - Known Plaintext
      - Hill...
      - Single Column Transposition...
    - Manual Analysis
      - Substitution...
      - Playfair...
      - Solitaire...
  - Symmetric Encryption (modern)
    - IDEA...
    - RC2...
    - RC4...
    - DES (ECB)...
    - DES (CBC)...
    - Triple DES (ECB)...
    - Triple DES (CBC)...
    - Rijndael (AES)...
    - Further Algorithms
      - MARS...
      - RC6...
      - Serpent...
      - Twofish...
      - DESX...
      - DESL...
      - DESXL...
  - Asymmetric Encryption
    - Factorization of a Number...
    - Lattice Based Attacks on RSA
      - Factoring with a Hint...
      - Attack on Stereotyped Messages...
      - Attack on Small Secret Keys...
    - Side-Channel Attack on "Textbook RSA"...
  - Hash
    - Attack on the Hash Value of the Digital Signature...
  - Analyze Randomness
    - Frequency Test...
    - Poker Test...
    - Runs Test...
    - Serial Test...
    - FIPS PUB-140-1 Test Battery
    - Vitányi
    - 3D Visualization...
- **Options**
  - Plot Options...
  - Analysis Options...
  - Text Options...
  - Starting Options...
- **Window**
  - Cascade
  - Tile
  - Arrange Icons
  - Close All
- **Help**
  - Starting Page
  - Index
  - Scenarios (Tutorials)
  - Readme
  - Script
  - Presentation
  - About CrypTool...

CT1 Lots of Online Help



CT1 Future and Wishes

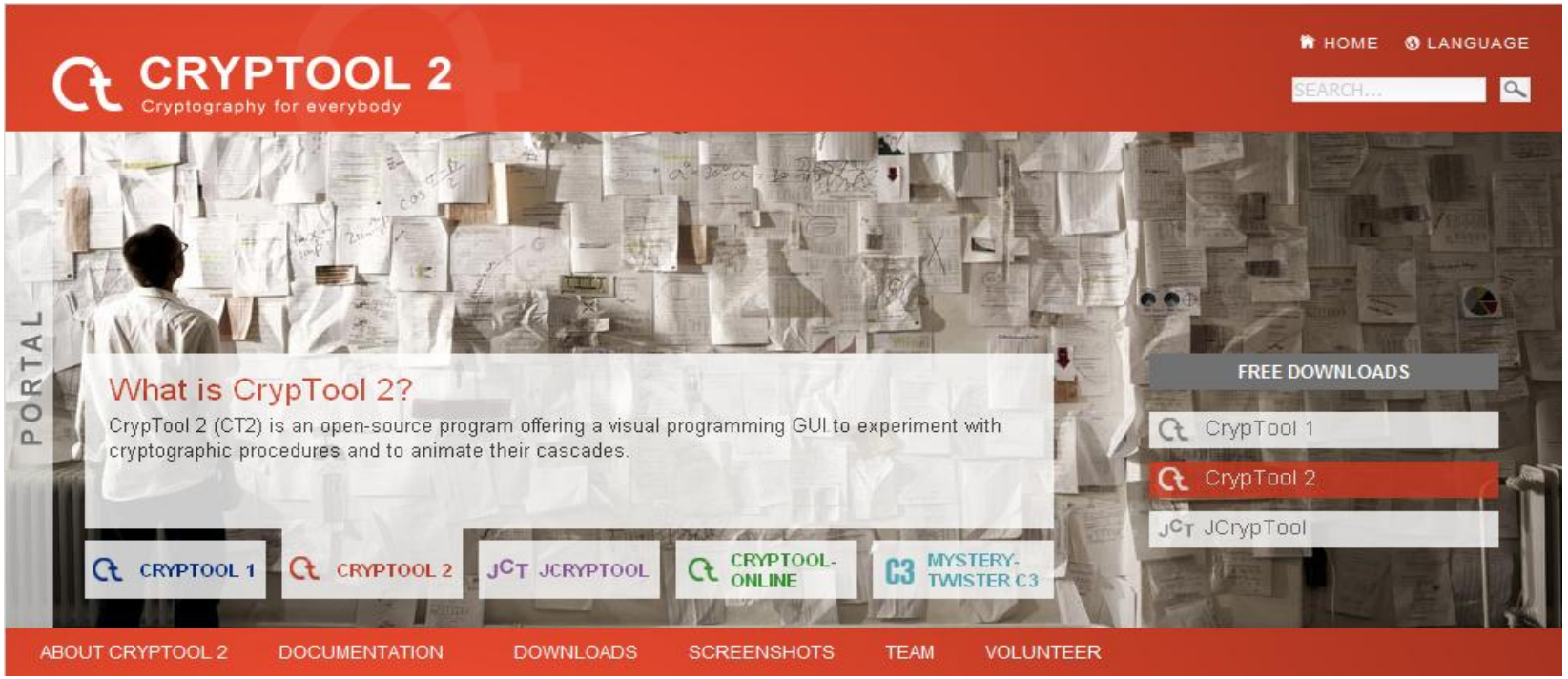
- Consistency and completeness
- Development assistance (programming, layout, translation, testing)
  - For the current C/C++ project
  - Mainly for the new projects (preferred):
    - C# project: “CrypTool 2.0“ = CT2
    - Java project: “JCrypTool“ = JCT
    - Browser project: “CrypTool-Online“ = CTO
- CT1 will be maintained, but new features will be added only to CT2 and JCT.
- CT1 is currently downloaded over 6000 times per month from the CrypTool website.

  - Just over half of these downloads are of the English version.

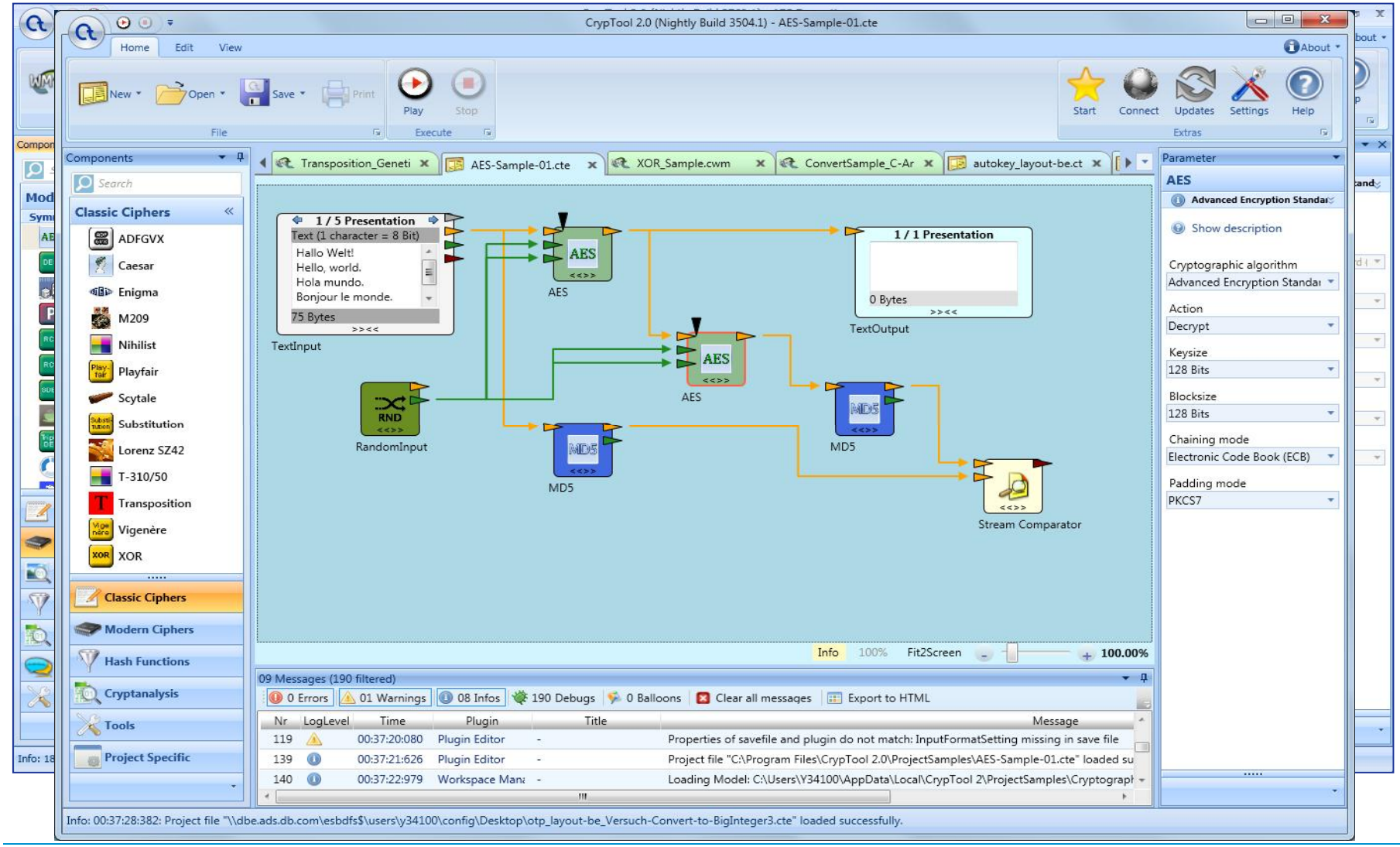
  - The betas CT2 and JCT are downloaded over 1000 times a month each.

CT2
www.cryptool.org/en

- CrypTool 2 [(Beta 9 and nightly builds, both are stable), Release CT 2.0 planned for end 2013]
  - C# under Visual Studio 2010 (Express Edition) and WPF
  - Runs under Windows 7 and 8 (requires for runtime the .NET Framework v4.0)
  - Available in English and German. Build-in automatic upgrade mechanism.



Example of modern symmetric encryption (AES) in CT2



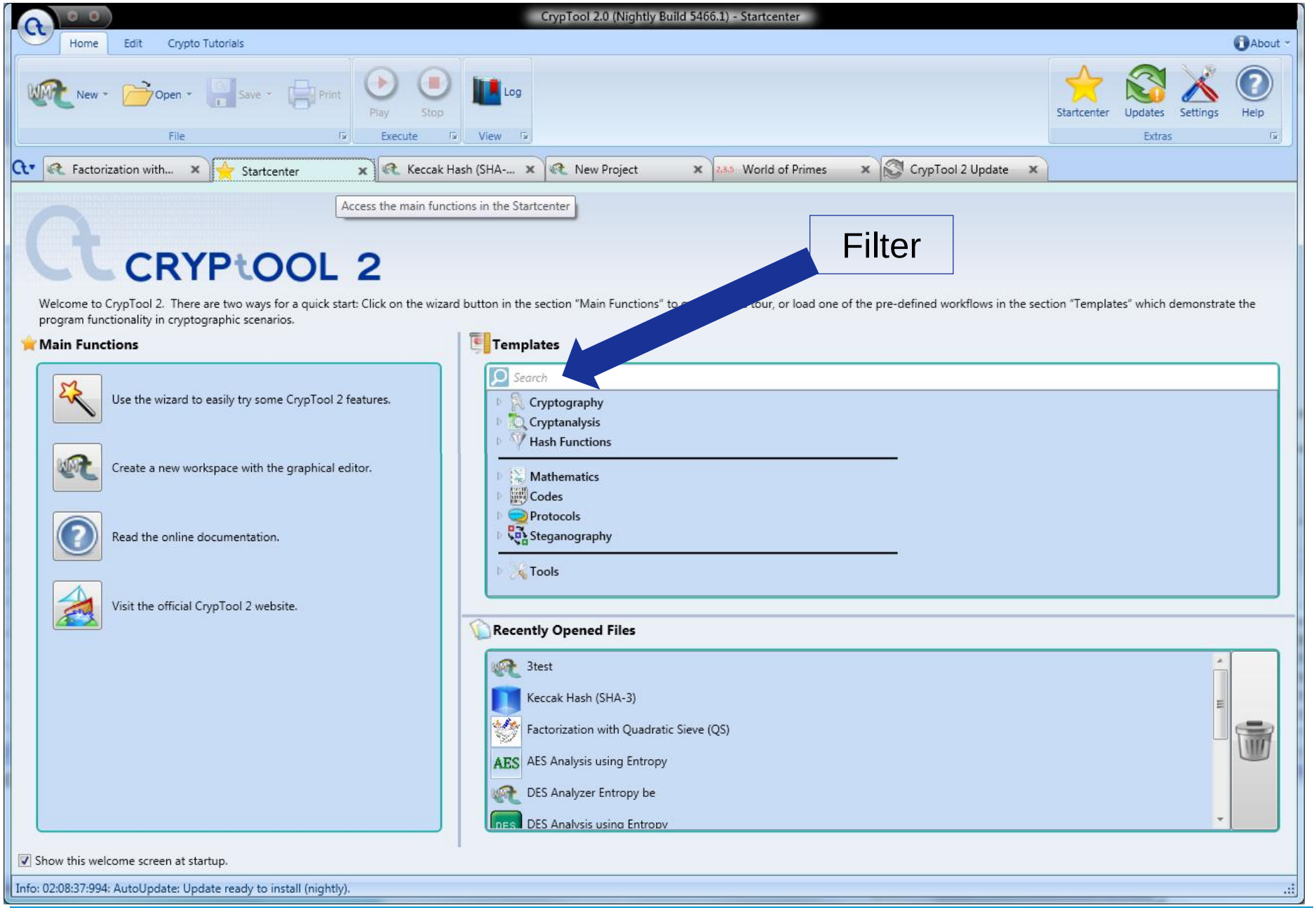
CT2 Features (1)

- Visual programming
  - Allows the combination of cryptographic and cryptanalytic components
  - Implicit data conversion (plus explicit conversion using converters)
  - CT2 learns which links are used more frequent when setting up a workflow (e.g. Caesar always suggests a test input and a text output component)
  - IControl enhances the components directly (much faster than via the GUI). It's like an additional card on a motherboard.
  - Components can include a visualization which can be shown within a window directly on the workplace. This allows to visualize several algorithms in "parallel".
- Classical and modern primitives, and protocols
  - Some have nice visuals like Enigma, PRESENT, Keccak, MD5, transposition, frequency analysis, (N)LFSR, Quadratic Sieve, Key Searcher, QR codes, Padding Oracle Attack
- Tutorial
  - Further people are needed to create videos we want to show directly within CT2
- Link with information for developing new plugins: http://www.cryptool.org/en/ct2-documentation-en

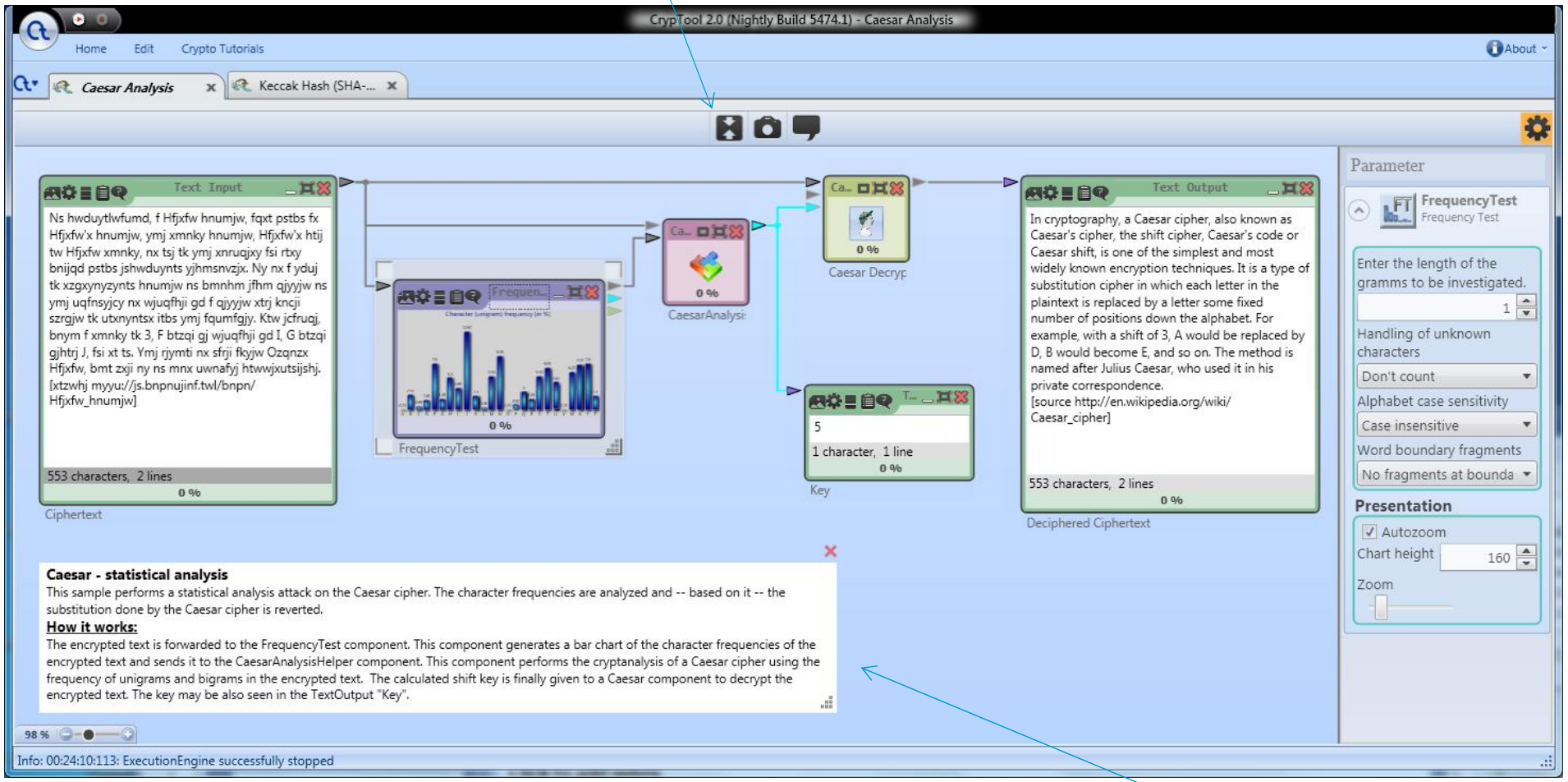
CT2 Features (2)

- Networking components supporting TCP / UDP
  - Components allow different participants at different computers to perform a protocol
  - Webcam encryption with and without DH
- GNFS (msieve enhanced to work multi-threaded; under construction)
- Framework for Research (to embed your research topic)
  - E-learning / didactics: How to use the new mechanisms, how to try new things?
  - Use the existing tools with all its elements (editor, interfaces, …) to test and discuss new methods (ciphers or attacks)
  - Volunteer Computing, e.g. for distributed cryptanalysis
    - Including a P2P network is planned for CT 2.1
- Teaching
  - Used in schools (pupils crypto courses, maths and computer science) and universities
  - Present crypto more accessible and easier to understand

Demo

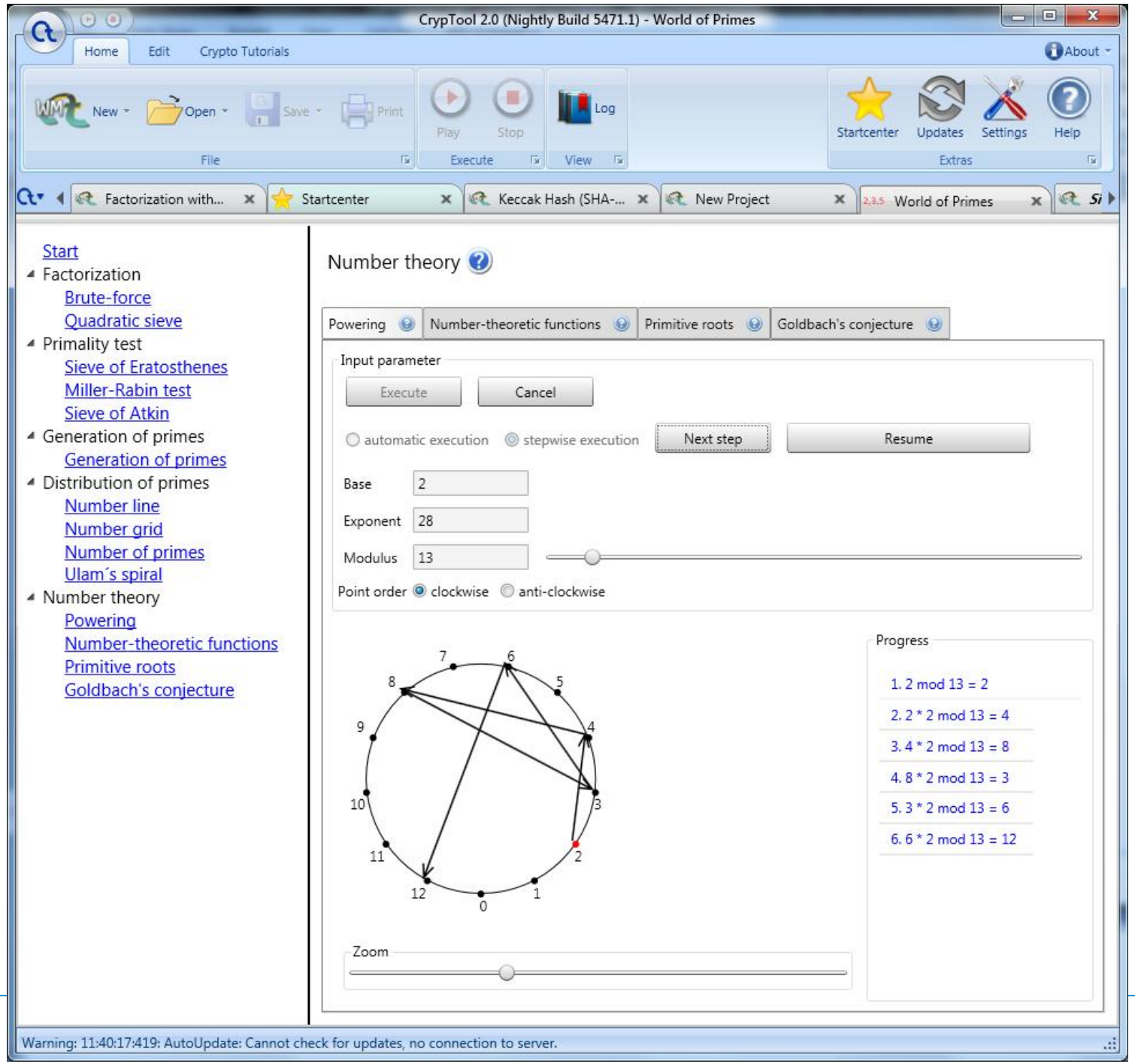

CrypTool 2.0 (Nightly Build 5466.1) - Startcenter
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
File
Play
Stop
Execute
Log
View
Startcenter
Updates
Settings
Help
Extras
Factorization with...
Startcenter
Keccak Hash (SHA-...
New Project
World of Primes
CrypTool 2 Update
Access the main functions in the Startcenter
CRYPTOOL 2
Filter
Welcome to CrypTool 2. There are two ways for a quick start: Click on the wizard button in the section "Main Functions" to
tour, or load one of the pre-defined workflows in the section "Templates" which demonstrate the program functionality in cryptographic scenarios.
Main Functions
Use the wizard to easily try some CrypTool 2 features.
Create a new workspace with the graphical editor.
Read the online documentation.
Visit the official CrypTool 2 website.
Templates
Search
Cryptography
Cryptanalysis
Hash Functions
Mathematics
Codes
Protocols
Steganography
Tools
Recently Opened Files
3test
Keccak Hash (SHA-3)
Factorization with Quadratic Sieve (QS)
AES Analysis using Entropy
DES Analyzer Entropy be
DES Analysis using Entropy
Show this welcome screen at startup.
Info: 02:08:37:994: AutoUpdate: Update ready to install (nightly).

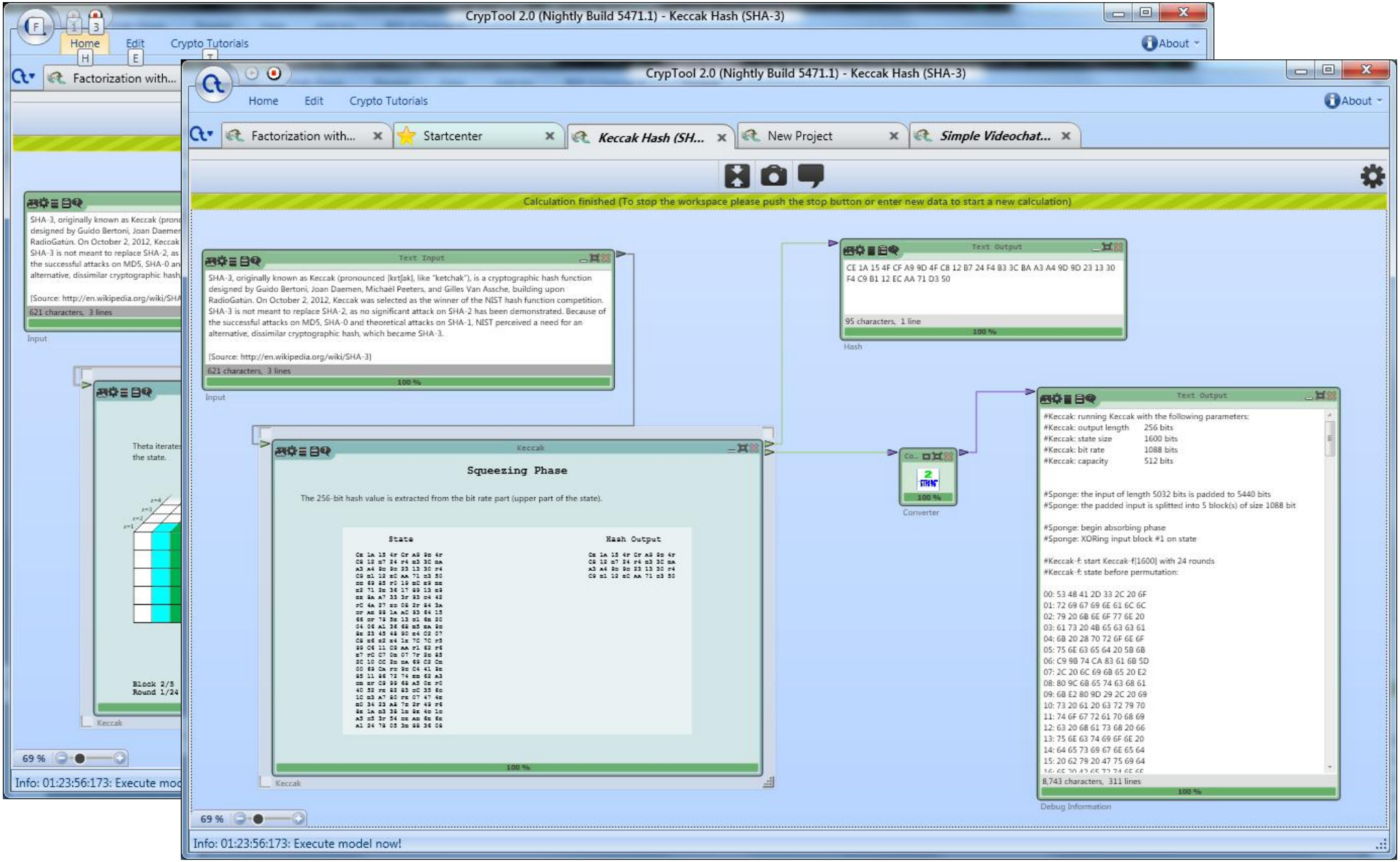
CT2

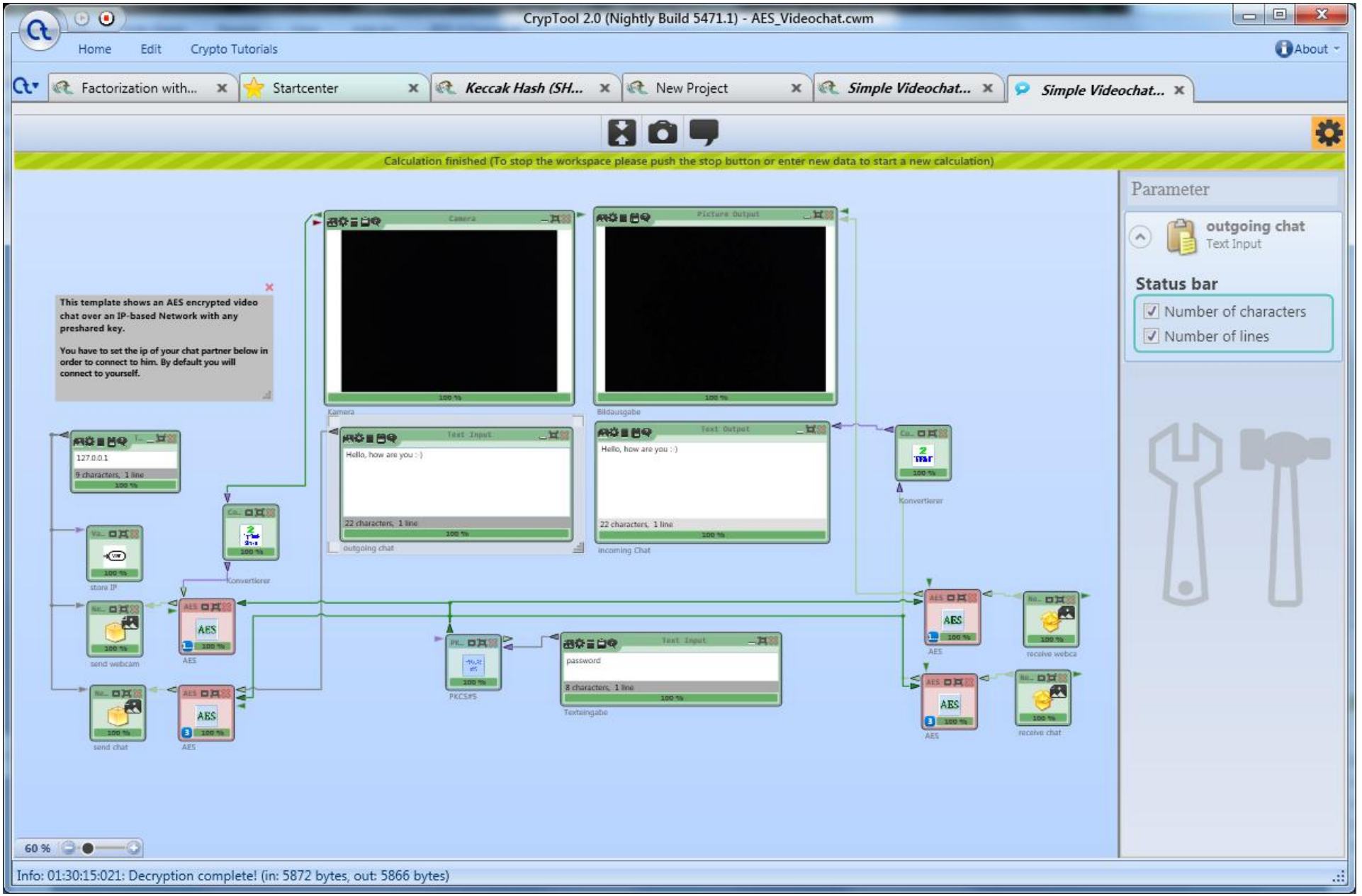


Quickly adapt the CT2 GUI with F11 and F12.

CT2


CrypTool 2.0 (Nightly Build 5471.1) - World of Primes
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
Startcenter
Updates
Settings
Help
File
Execute
View
Extras
Factorization with...
Startcenter
Keccak Hash (SHA-...
New Project
World of Primes
Start
Factorization
Brute-force
Quadratic sieve
Primality test
Sieve of Eratosthenes
Miller-Rabin test
Sieve of Atkin
Generation of primes
Generation of primes
Distribution of primes
Number line
Number grid
Number of primes
Ulam´s spiral
Number theory
Powering
Number-theoretic functions
Primitive roots
Goldbach's conjecture
Number theory
Powering
Number-theoretic functions
Primitive roots
Goldbach's conjecture
Input parameter
Execute
Cancel
automatic execution
stepwise execution
Next step
Resume
Base
2
Exponent
28
Modulus
13
Point order
clockwise
anti-clockwise
Progress
1. 2 mod 13 = 2
2. 2 * 2 mod 13 = 4
3. 4 * 2 mod 13 = 8
4. 8 * 2 mod 13 = 3
5. 3 * 2 mod 13 = 6
6. 6 * 2 mod 13 = 12
Zoom
Warning: 11:40:17:419: AutoUpdate: Cannot check for updates, no connection to server.

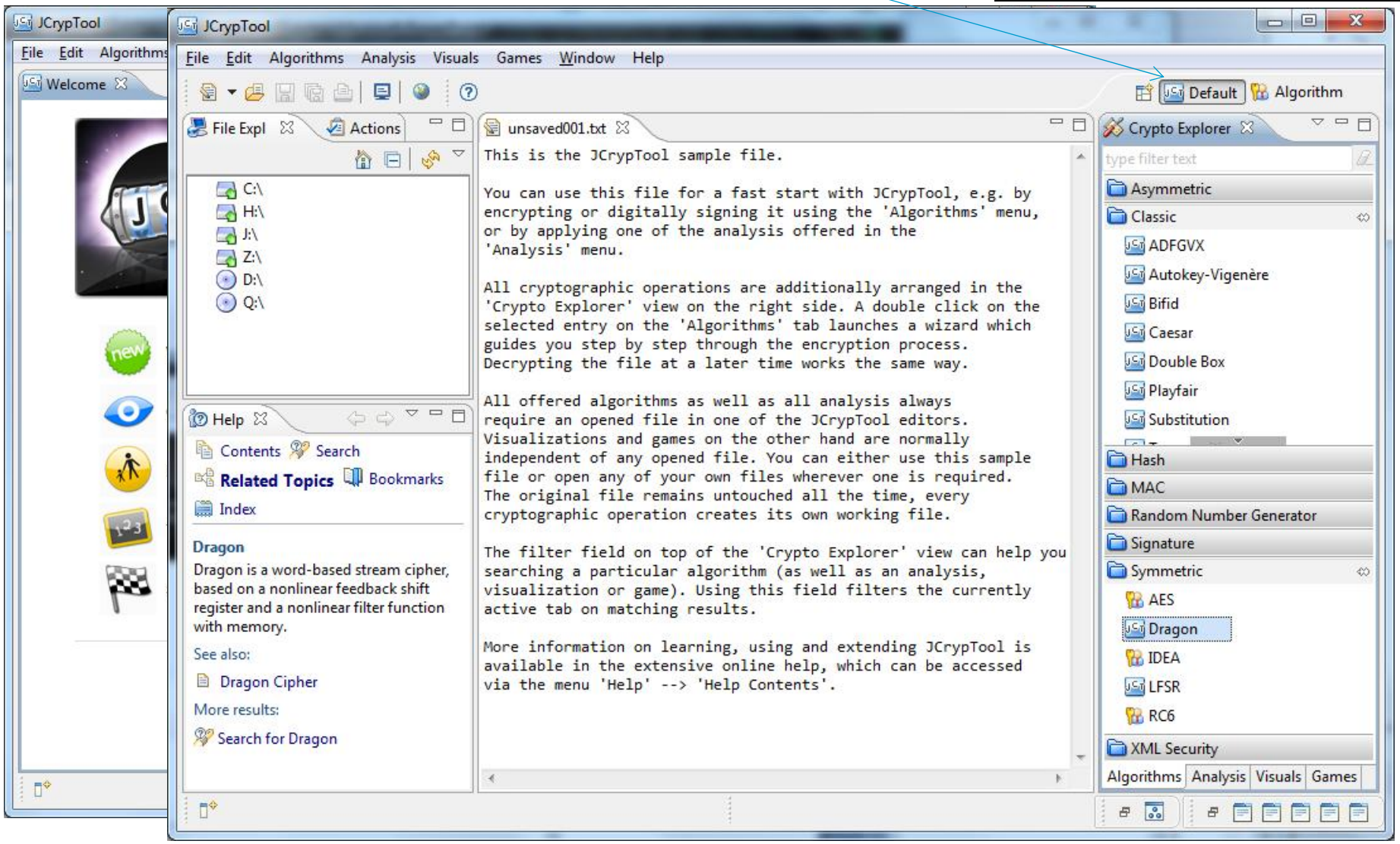

CrypTool 2.0 (Nightly Build 5471.1) - Keccak Hash (SHA-3)
Home
Edit
Crypto Tutorials
About
Factorization with...
Startcenter
Keccak Hash (SH...
New Project
Simple Videochat...
Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)
Text Input
SHA-3, originally known as Keccak (pronounced [krtʃak], like "ketchak"), is a cryptographic hash function designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, building upon RadioGatún. On October 2, 2012, Keccak was selected as the winner of the NIST hash function competition. SHA-3 is not meant to replace SHA-2, as no significant attack on SHA-2 has been demonstrated. Because of the successful attacks on MD5, SHA-0 and theoretical attacks on SHA-1, NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3.
[Source: http://en.wikipedia.org/wiki/SHA-3]
621 characters, 3 lines
100 %
Input
Text Output
CE 1A 15 4F CF A9 9D 4F C8 12 B7 24 F4 B3 3C BA A3 A4 9D 9D 23 13 30 F4 C9 B1 12 EC AA 71 D3 50
95 characters, 1 line
100 %
Hash
Keccak
Squeezing Phase
The 256-bit hash value is extracted from the bit rate part (upper part of the state).
State
Hash Output
Converter
Text Output
#Keccak: running Keccak with the following parameters:
#Keccak: output length 256 bits
#Keccak: state size 1600 bits
#Keccak: bit rate 1088 bits
#Keccak: capacity 512 bits
#Sponge: the input of length 5032 bits is padded to 5440 bits
#Sponge: the padded input is splitted into 5 block(s) of size 1088 bit
#Sponge: begin absorbing phase
#Sponge: XORing input block #1 on state
#Keccak-f: start Keccak-f[1600] with 24 rounds
#Keccak-f: state before permutation:
00: 53 48 41 2D 33 2C 20 6F
01: 72 69 67 69 6E 61 6C 6C
02: 79 20 6B 6E 6F 77 6E 20
03: 61 73 20 4B 65 63 63 61
04: 6B 20 28 70 72 6F 6E 6F
05: 75 6E 63 65 64 20 5B 6B
06: C9 9B 74 CA 83 61 6B 5D
07: 2C 20 6C 69 6B 65 20 E2
08: 80 9C 6B 65 74 63 68 61
09: 6B E2 80 9D 29 2C 20 69
10: 73 20 61 20 63 72 79 70
11: 74 6F 67 72 61 70 68 69
12: 63 20 6B 61 73 68 20 66
13: 75 6E 63 74 69 6F 6E 20
14: 64 65 73 69 67 6E 65 64
15: 20 62 79 20 47 75 69 64
8,743 characters, 311 lines
100 %
Debug Information
69 %
Info: 01:23:56:173: Execute model now!


CrypTool 2.0 (Nightly Build 5471.1) - AES_Videochat.cwm
Home
Edit
Crypto Tutorials
About
Factorization with...
Startcenter
Keccak Hash (SH...
New Project
Simple Videochat...
Simple Videochat...
Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)
This template shows an AES encrypted video chat over an IP-based Network with any preshared key.
You have to set the ip of your chat partner below in order to connect to him. By default you will connect to yourself.
Camera
Picture Output
Kamera
Bildausgabe
127.0.0.1
9 characters, 1 line
Text Input
Hello, how are you :)
22 characters, 1 line
outgoing chat
Text Output
Hello, how are you :)
22 characters, 1 line
incoming Chat
Konvertierer
store IP
send webcam
AES
PKCS#5
password
8 characters, 1 line
Texteingabe
receive webca
receive chat
send chat
Parameter
outgoing chat
Text Input
Status bar
Number of characters
Number of lines
60 %
Info: 01:30:15:021: Decryption complete! (in: 5872 bytes, out: 5866 bytes)

JCT
www.cryptool.org/en

- JCrypTool [RC 6 and weekly builds (both are stable), Release JCT 1.0 planned for end 2013]
  - Java with Eclipse RCP and SWT; runs on Windows, MacOS and Linux
  - Available in English and German
  - Build-in automatic upgrade mechanism

JCT – Welcome and **Default Perspective**



JCT Features

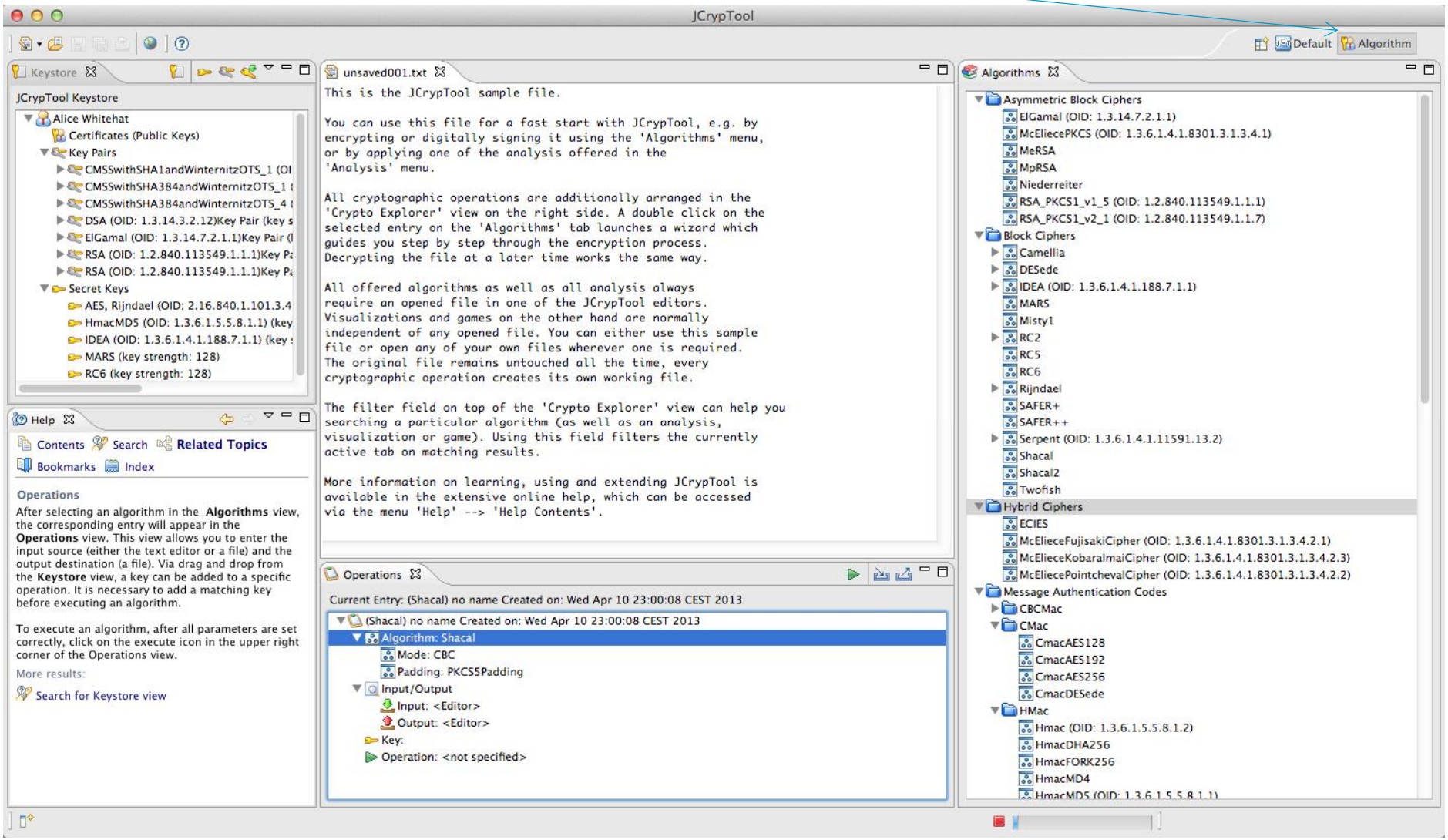
- Platform independent
  - Delivered by Eclipse (RCP), a crypto plugin developer doesn't have to care. He just develops on his platform.
- Two perspectives (Default and Algorithm)
- Two crypto providers (FP, BC)
- Text and hex editor
- Visualizations
- Cascading of ciphers
- Action history
- Common key store used by all modern plugins.
  It stores secret and public keys, certificates and some meta data.
- Work in progress: e.g. integration of BicliqueFinder, a PKI, …
- Link with information for developing new plugins:
  https://github.com/jcryptool/core/wiki

These features plus a modern GUI are offered by JCT.

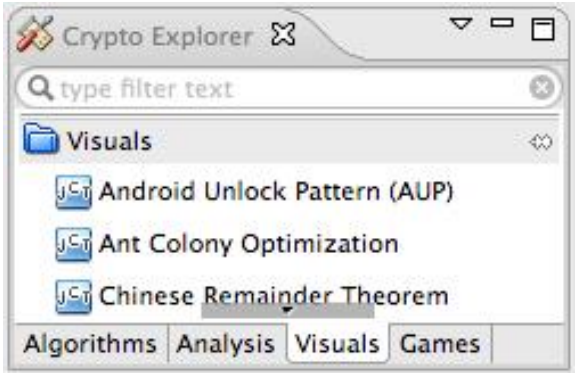
The crypto-plugin developer decides what to use.

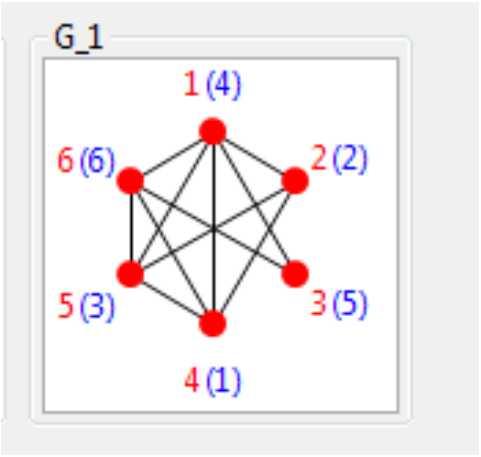
Demo

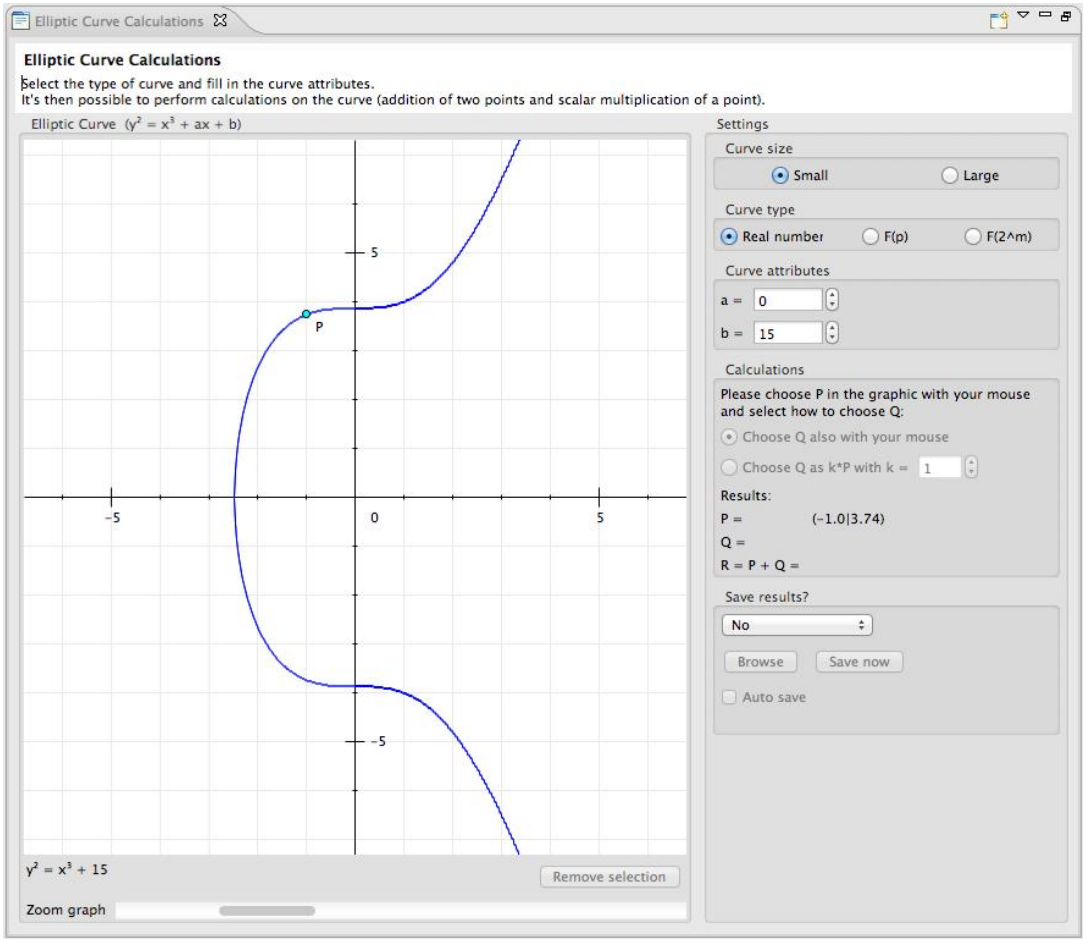
JCT – **Algorithm Perspective**



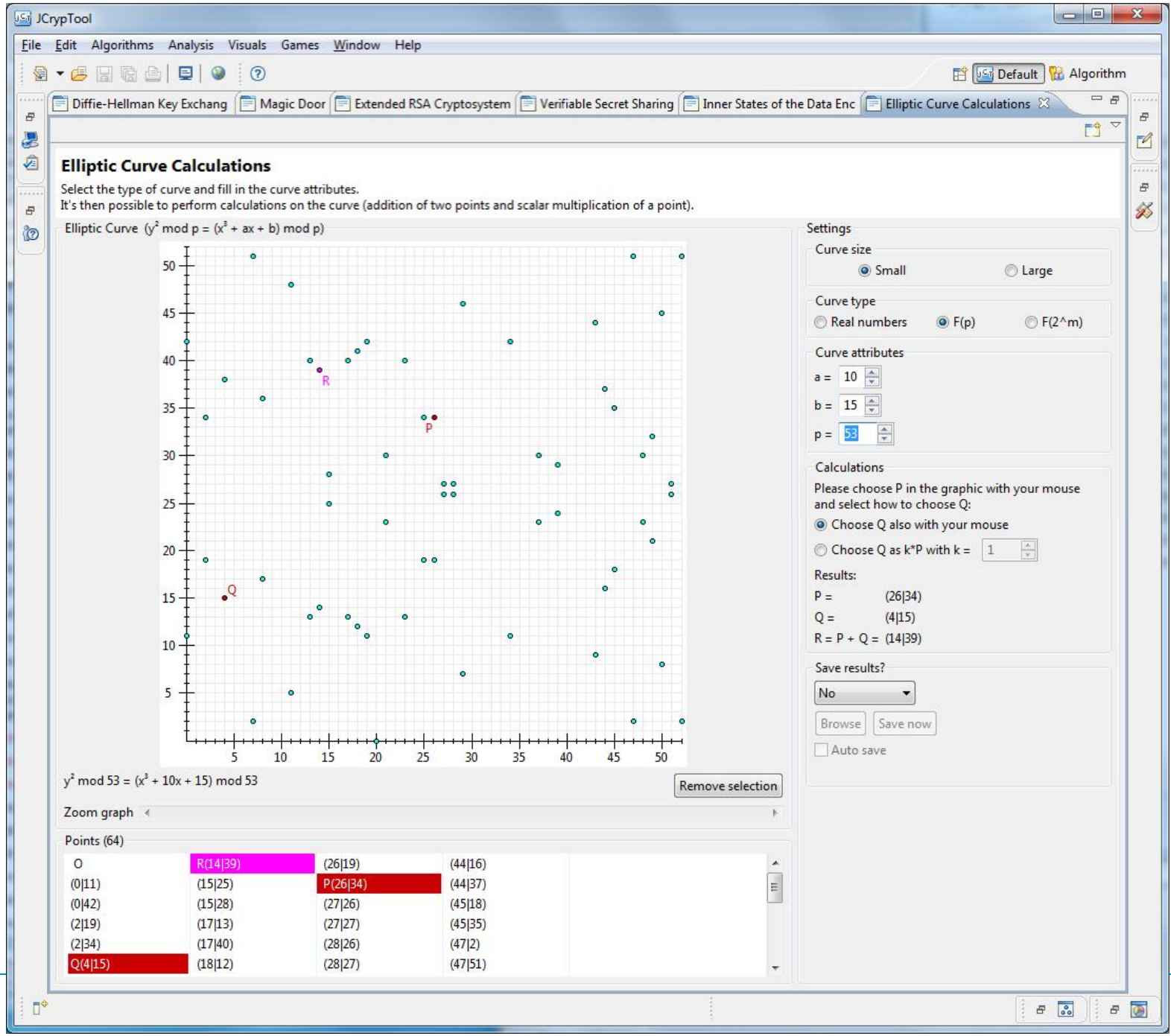
JCT


Crypto Explorer
type filter text
Visuals
Android Unlock Pattern (AUP)
Ant Colony Optimization
Chinese Remainder Theorem
Algorithms
Analysis
Visuals
Games


G_1
1 (4)
6 (6)
2 (2)
5 (3)
3 (5)
4 (1)


Elliptic Curve Calculations
Elliptic Curve Calculations
Select the type of curve and fill in the curve attributes.
It's then possible to perform calculations on the curve (addition of two points and scalar multiplication of a point).
Elliptic Curve (y² = x³ + ax + b)
Settings
Curve size
Small
Large
Curve type
Real number
F(p)
F(2^m)
Curve attributes
a = 0
b = 15
Calculations
Please choose P in the graphic with your mouse and select how to choose Q:
Choose Q also with your mouse
Choose Q as k*P with k = 1
Results:
P = (-1.0|3.74)
Q =
R = P + Q =
Save results?
No
Browse
Save now
Auto save
P
5
-5
0
5
-5
y² = x³ + 15
Remove selection
Zoom graph

JCT


JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
Default Algorithm
Diffie-Hellman Key Exchang
Magic Door
Extended RSA Cryptosystem
Verifiable Secret Sharing
Inner States of the Data Enc
Elliptic Curve Calculations
Elliptic Curve Calculations
Select the type of curve and fill in the curve attributes.
It's then possible to perform calculations on the curve (addition of two points and scalar multiplication of a point).
Elliptic Curve (y² mod p = (x³ + ax + b) mod p)
R
P
Q
y² mod 53 = (x³ + 10x + 15) mod 53
Remove selection
Zoom graph
Points (64)
O
(0|11)
(0|42)
(2|19)
(2|34)
Q(4|15)
R(14|39)
(15|25)
(15|28)
(17|13)
(17|40)
(18|12)
(26|19)
P(26|34)
(27|26)
(27|27)
(28|26)
(28|27)
(44|16)
(44|37)
(45|18)
(45|35)
(47|2)
(47|51)
Settings
Curve size
Small
Large
Curve type
Real numbers
F(p)
F(2^m)
Curve attributes
a = 10
b = 15
p = 53
Calculations
Please choose P in the graphic with your mouse and select how to choose Q:
Choose Q also with your mouse
Choose Q as k*P with k = 1
Results:
P = (26|34)
Q = (4|15)
R = P + Q = (14|39)
Save results?
No
Browse
Save now
Auto save

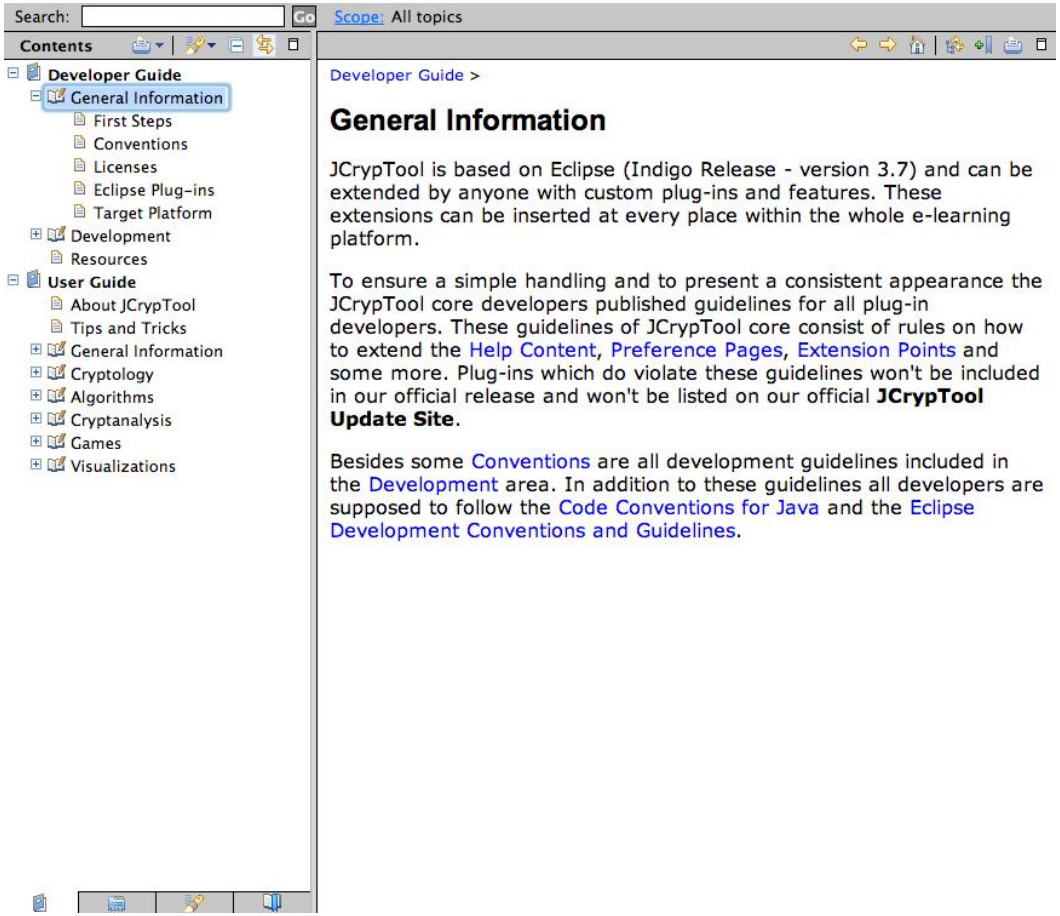
JCT Information for Developers

Wiki: https://github.com/jcryptool/core/wiki

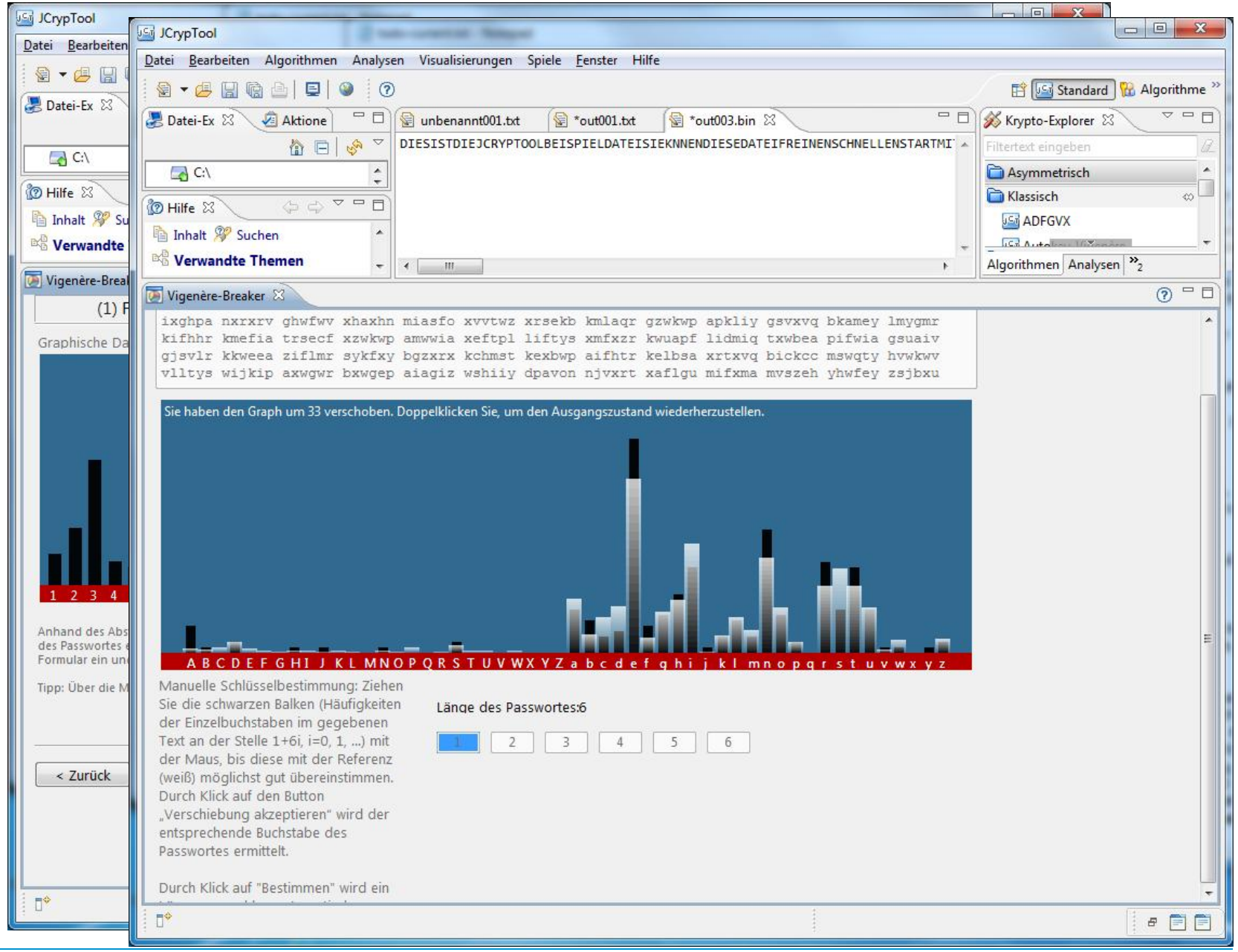
Style-Guide: https://github.com/jcryptool/doc/blob/master/Guidelines/JCrypTool-GUI-Guidelines.pdf

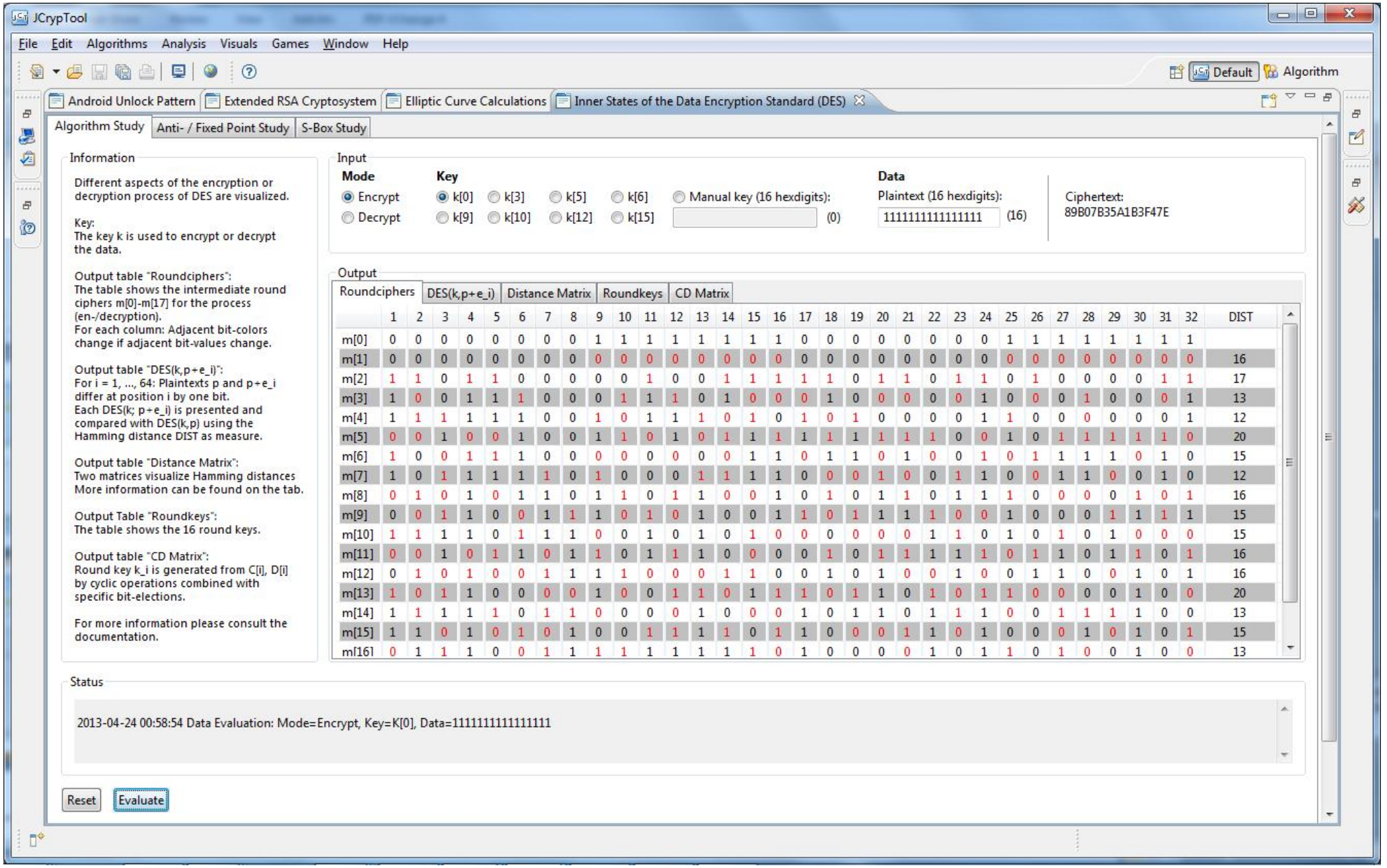
Information for developing plugins is provided in the **JCT online help** (analog to Eclipse).

The **wiki in the Internet** offers links and information for JCT-core developer or current issues, which after a release could not be included in the online help. Plugin developers should not need any projects from the JCT repository but need to run JCT as a target platform and develop for it.



JCT


JCrypTool
Datei Bearbeiten Algorithmen Analysen Visualisierungen Spiele Fenster Hilfe
Standard
Algorithme
Datei-Ex
Aktione
C:\
Hilfe
Inhalt Suchen
Verwandte Themen
unbenannt001.txt
*out001.txt
*out003.bin
DIESISTDIEJCRYPTOOLBEISPIELDATEISIEKNNENDIESEDATEIFREINENSCHNELLENSTARTMI
Krypto-Explorer
Filtertext eingeben
Asymmetrisch
Klassisch
ADFGVX
Algorithmen
Analysen
Vigenère-Breaker
ixghpa nxrxrv ghwfwv xhaxhn miasfo xvvtwz xrsekb kmlaqr gzwkwp apkliy gsvxvq bkamey lmygmr
kifhhr kmefia trsecf xzwkwp amwwia xeftpl liftys xmfxzr kwuapf lidmiq txwbea pifwia gsuaiv
gjsvlr kkweea ziflmr sykfxy bgzxrx kchmst kexbwp aifhtr kelbsa xrtxvq bickcc mswqty hvwkwv
vlltys wijkip axwgwr bxwgep aiagiz wshiiy dpavon njvxrt xaflgu mifxma mvszeh yhwfey zsjbxu
Sie haben den Graph um 33 verschoben. Doppelklicken Sie, um den Ausgangszustand wiederherzustellen.
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
Manuelle Schlüsselbestimmung: Ziehen Sie die schwarzen Balken (Häufigkeiten der Einzelbuchstaben im gegebenen Text an der Stelle 1+6i, i=0, 1, ...) mit der Maus, bis diese mit der Referenz (weiß) möglichst gut übereinstimmen. Durch Klick auf den Button „Verschiebung akzeptieren" wird der entsprechende Buchstabe des Passwortes ermittelt.
Durch Klick auf "Bestimmen" wird ein
Länge des Passwortes:6
1 2 3 4 5 6
Graphische Da
1 2 3 4
Anhand des Abs
des Passwortes
Formular ein un
Tipp: Über die M
< Zurück



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	DIST
m[0]	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	
m[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16
m[2]	1	1	0	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	1	0	1	0	0	0	0	1	1	17
m[3]	1	0	0	1	1	1	0	0	0	1	1	1	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	1	13
m[4]	1	1	1	1	1	1	0	0	1	0	1	1	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	1	12
m[5]	0	0	1	0	0	1	0	0	1	1	0	1	0	1	1	1	1	1	1	1	1	1	0	0	1	0	1	1	1	1	1	0	20
m[6]	1	0	0	1	1	1	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1	1	1	0	1	0	15
m[7]	1	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	0	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	12
m[8]	0	1	0	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	0	0	1	0	1	16
m[9]	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	1	1	0	1	1	1	1	0	0	1	0	0	0	1	1	1	1	15
m[10]	1	1	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1	1	0	1	0	1	0	1	0	0	0	15
m[11]	0	0	1	0	1	1	0	1	1	0	1	1	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	0	1	16
m[12]	0	1	0	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	16
m[13]	1	0	1	1	0	0	0	0	1	0	0	1	1	0	1	1	1	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0	20
m[14]	1	1	1	1	1	0	1	1	0	0	0	0	1	0	0	0	1	0	1	1	0	1	1	1	0	0	1	1	1	1	0	0	13
m[15]	1	1	0	1	0	1	0	1	0	0	1	1	1	1	0	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1	0	1	15
m[16]	0	1	1	1	0	0	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	0	1	1	0	1	0	0	1	0	0	13

Sub Agenda

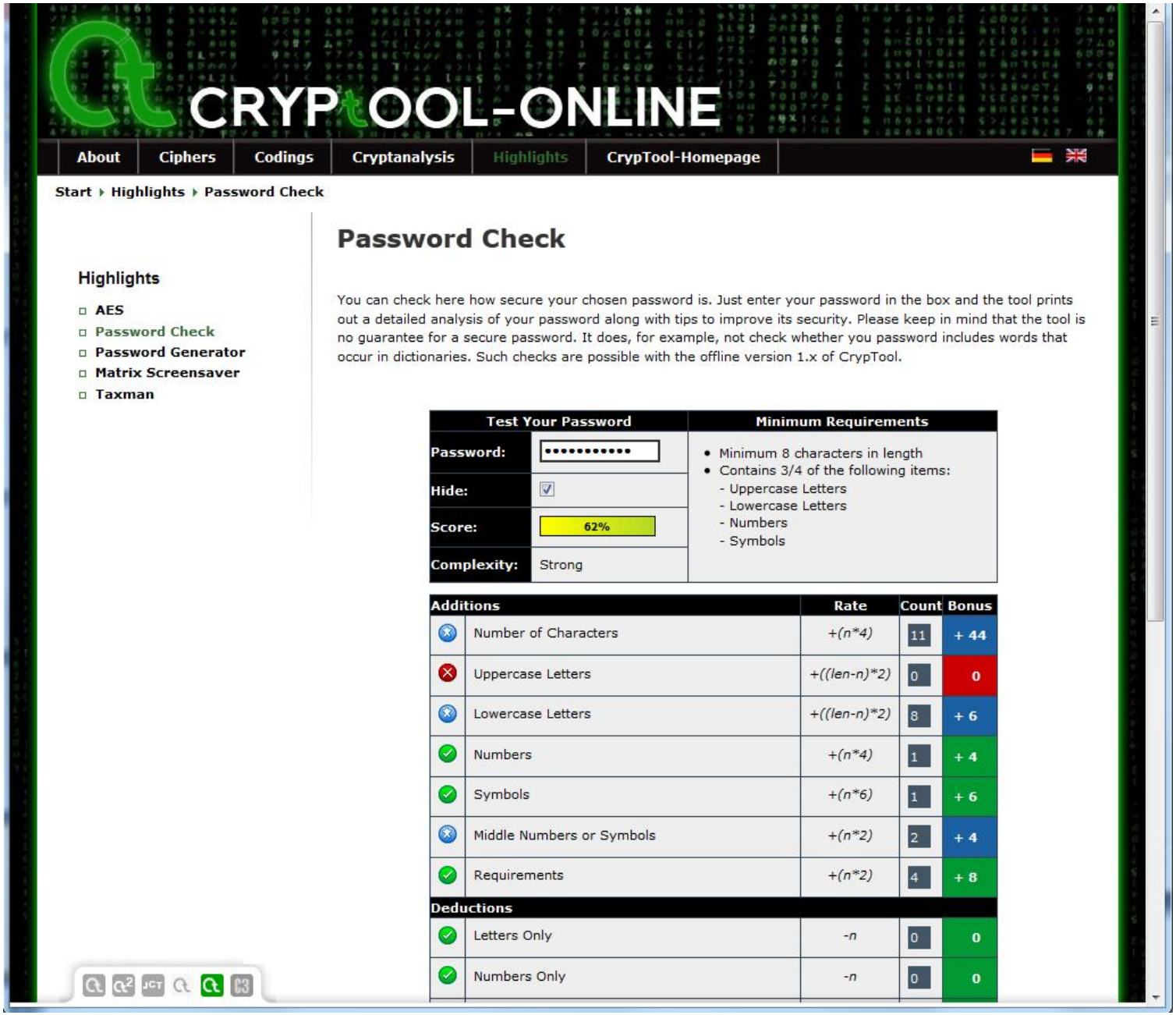
1	Why we created CrypTool
2	Context and basics of cryptography
3	Cryptography with the offline programs CT1, CT2 and JCT
4	CT websites: CTP (CT Portal), CTO (CrypTool Online), MTC3

Online Resource: CTO
www.cryptool.org/en

- CrypTool-Online
  - CrypTool within a browser (running on a PC or on a smart phone)
  - Available in English and German

CTO: http://www.cryptool-online.org

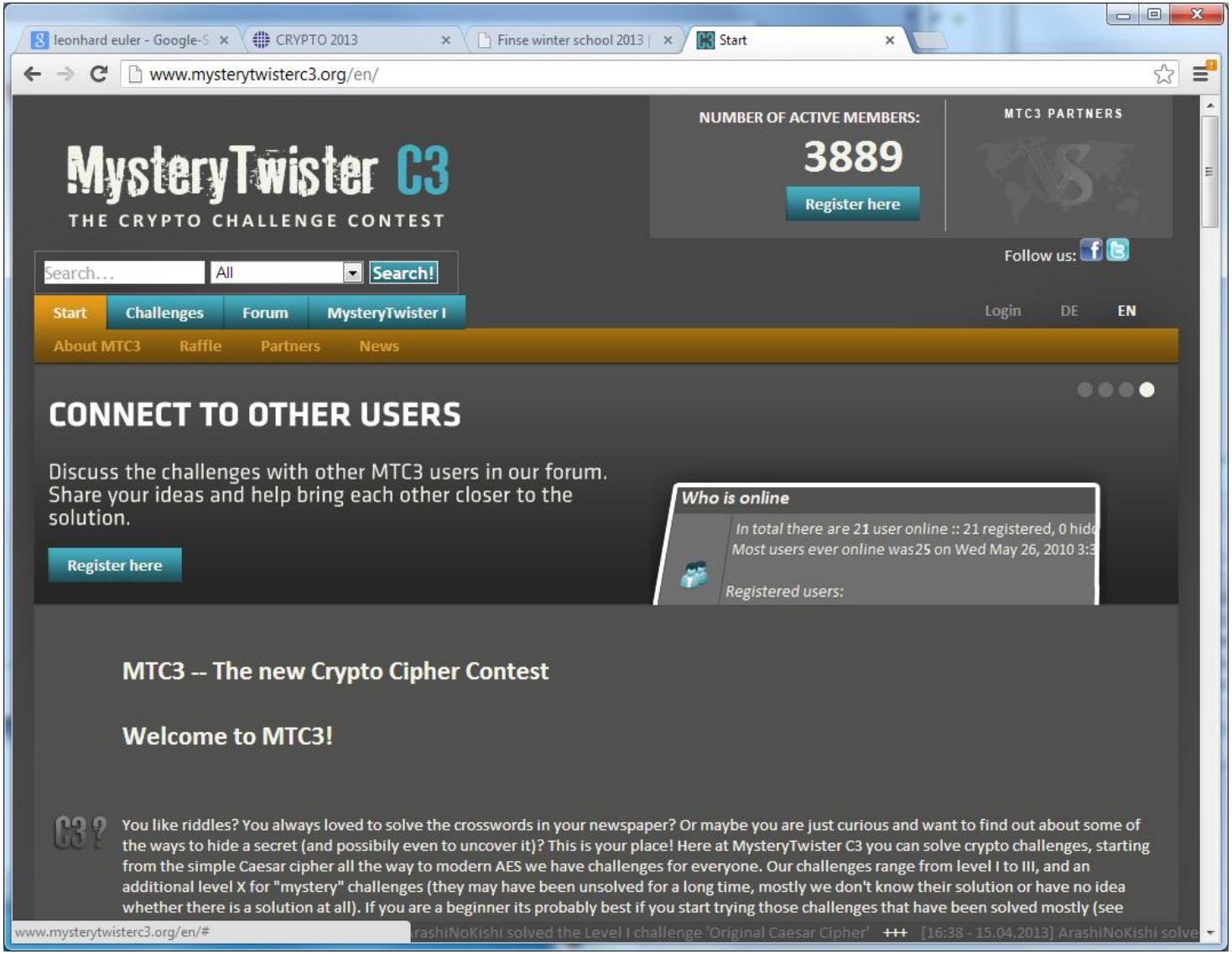
CTO:


CRYPTOOL-ONLINE
About
Ciphers
Codings
Cryptanalysis
Highlights
CrypTool-Homepage
Start ▸ Highlights ▸ Password Check
Highlights
AES
Password Check
Password Generator
Matrix Screensaver
Taxman
Password Check
You can check here how secure your chosen password is. Just enter your password in the box and the tool prints out a detailed analysis of your password along with tips to improve its security. Please keep in mind that the tool is no guarantee for a secure password. It does, for example, not check whether you password includes words that occur in dictionaries. Such checks are possible with the offline version 1.x of CrypTool.
Test Your Password
Password:
Hide:
Score:
62%
Complexity:
Strong
Minimum Requirements
Minimum 8 characters in length
Contains 3/4 of the following items:
- Uppercase Letters
- Lowercase Letters
- Numbers
- Symbols
Additions
Rate
Count
Bonus
Number of Characters
+(n*4)
11
+ 44
Uppercase Letters
+((len-n)*2)
0
0
Lowercase Letters
+((len-n)*2)
8
+ 6
Numbers
+(n*4)
1
+ 4
Symbols
+(n*6)
1
+ 6
Middle Numbers or Symbols
+(n*2)
2
+ 4
Requirements
+(n*2)
4
+ 8
Deductions
Letters Only
-n
0
0
Numbers Only
-n
0
0

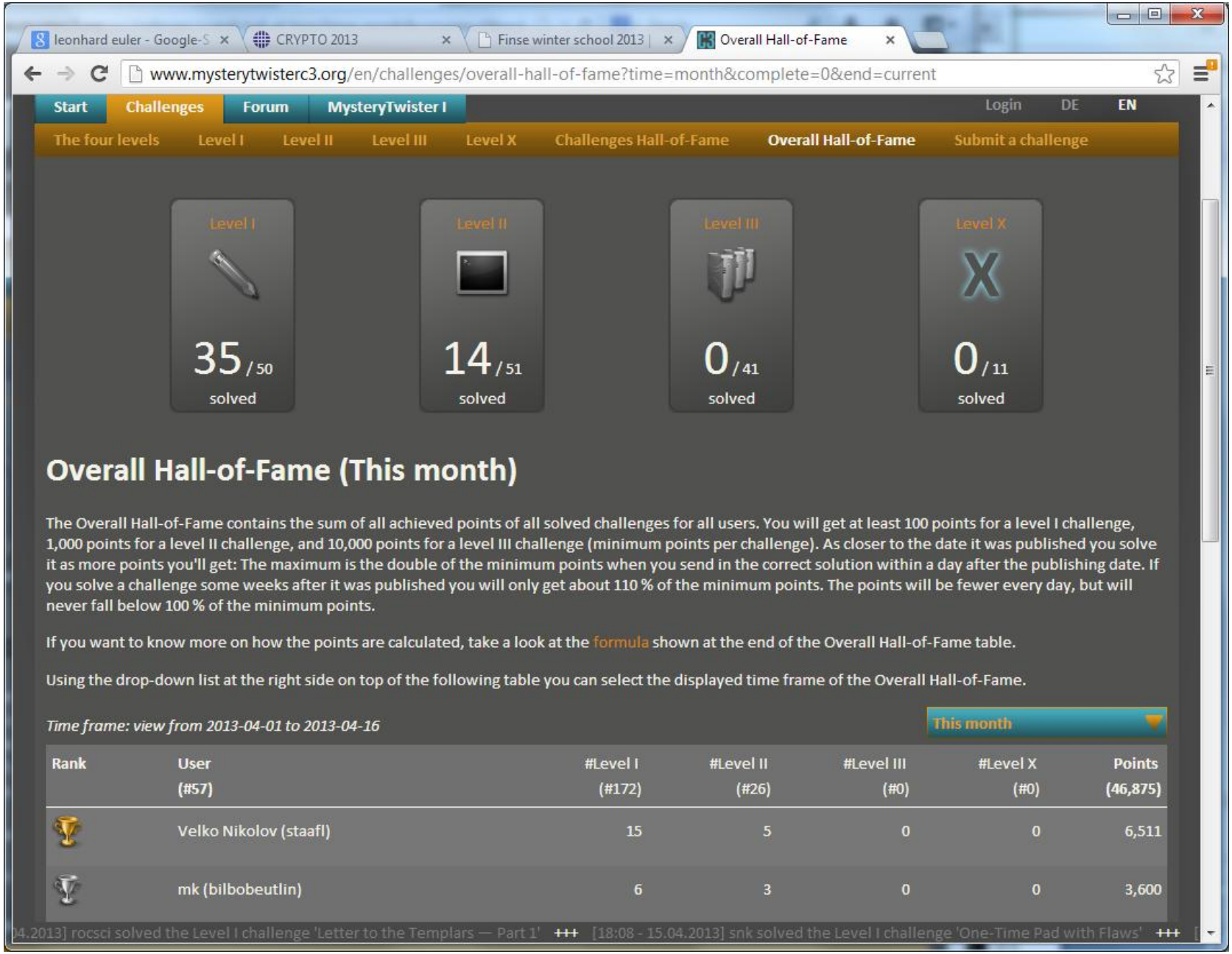
Online Resource: MTC3 – The Cipher Contest
www.cryptool.org/en

- MysteryTwister C3 (MTC3)
  - International Crypto Cipher Contest
  - Available in English and German
  - Currently more than 150 challenges, built by more than 36 different authors

MTC3: http://www.mysterytwisterc3.org/



MTC3:


leonhard euler - Google-S
CRYPTO 2013
Finse winter school 2013
Overall Hall-of-Fame
www.mysterytwisterc3.org/en/challenges/overall-hall-of-fame?time=month&complete=0&end=current
Start
Challenges
Forum
MysteryTwister I
Login
DE
EN
The four levels
Level I
Level II
Level III
Level X
Challenges Hall-of-Fame
Overall Hall-of-Fame
Submit a challenge
Level I
35 / 50
solved
Level II
14 / 51
solved
Level III
0 / 41
solved
Level X
0 / 11
solved
Overall Hall-of-Fame (This month)
The Overall Hall-of-Fame contains the sum of all achieved points of all solved challenges for all users. You will get at least 100 points for a level I challenge, 1,000 points for a level II challenge, and 10,000 points for a level III challenge (minimum points per challenge). As closer to the date it was published you solve it as more points you'll get: The maximum is the double of the minimum points when you send in the correct solution within a day after the publishing date. If you solve a challenge some weeks after it was published you will only get about 110 % of the minimum points. The points will be fewer every day, but will never fall below 100 % of the minimum points.
If you want to know more on how the points are calculated, take a look at the formula shown at the end of the Overall Hall-of-Fame table.
Using the drop-down list at the right side on top of the following table you can select the displayed time frame of the Overall Hall-of-Fame.
Time frame: view from 2013-04-01 to 2013-04-16
This month
Rank
User (#57)
#Level I (#172)
#Level II (#26)
#Level III (#0)
#Level X (#0)
Points (46,875)
Velko Nikolov (staafl) 15 5 0 0 6,511
mk (bilbobeutlin) 6 3 0 0 3,600
4.2013] rocsci solved the Level I challenge 'Letter to the Templars — Part 1' +++ [18:08 - 15.04.2013] snk solved the Level I challenge 'One-Time Pad with Flaws' +++

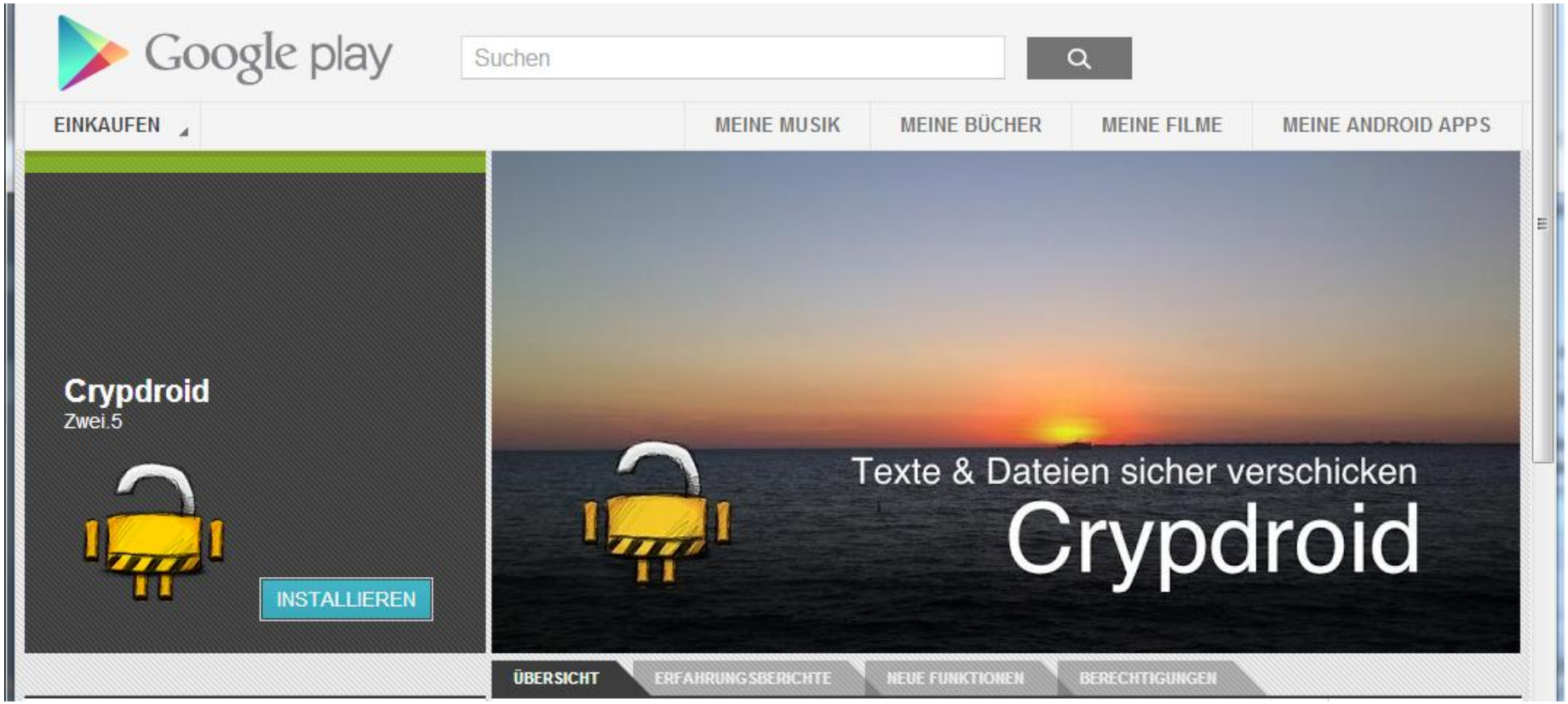
MTC3:

70 year old riddle from WW2 solved after being offered for 2 years in MTC3. Published April 22nd, 2013 in Spiegel-Online.

http://einestages.spiegel.de/s/tb/28303/geheimes-tagebuch-aus-dem-zweiten-weltkrieg-entschluesselt.html

Crypdroid: https://play.google.com/store/apps/details?id=de.zweipunktfuenf.crypdroid

Android App for secure encryption; scheme is compatible to CT2

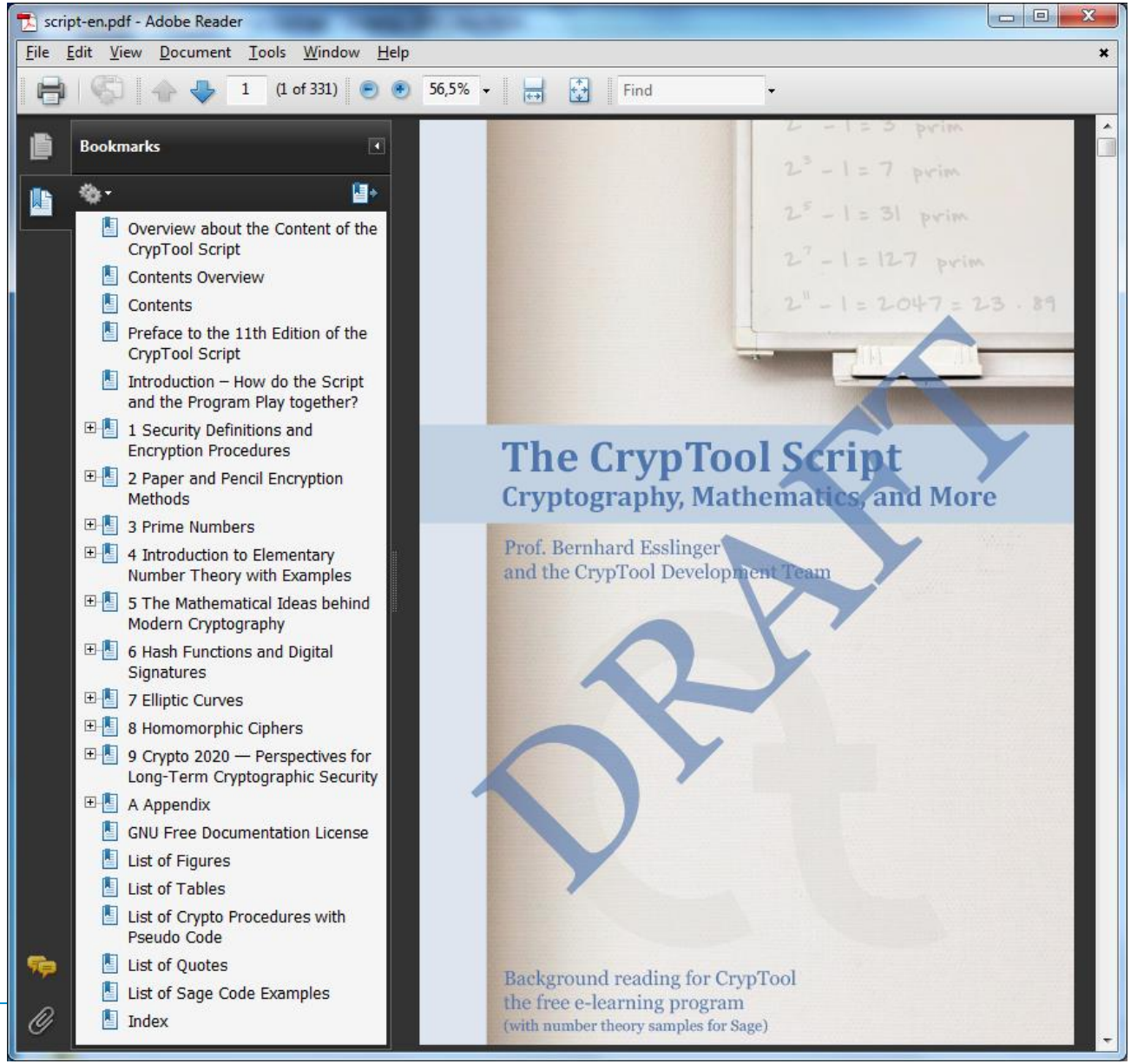


MTC3:
Current challenge especially for the participants in the Finse snow!

More Mathematical Background Information (incl. Sage): CrypTool Script

http://www.cryptool.org/en/ctp-documentation-en/ctp-script-en

(take the one from 2013)



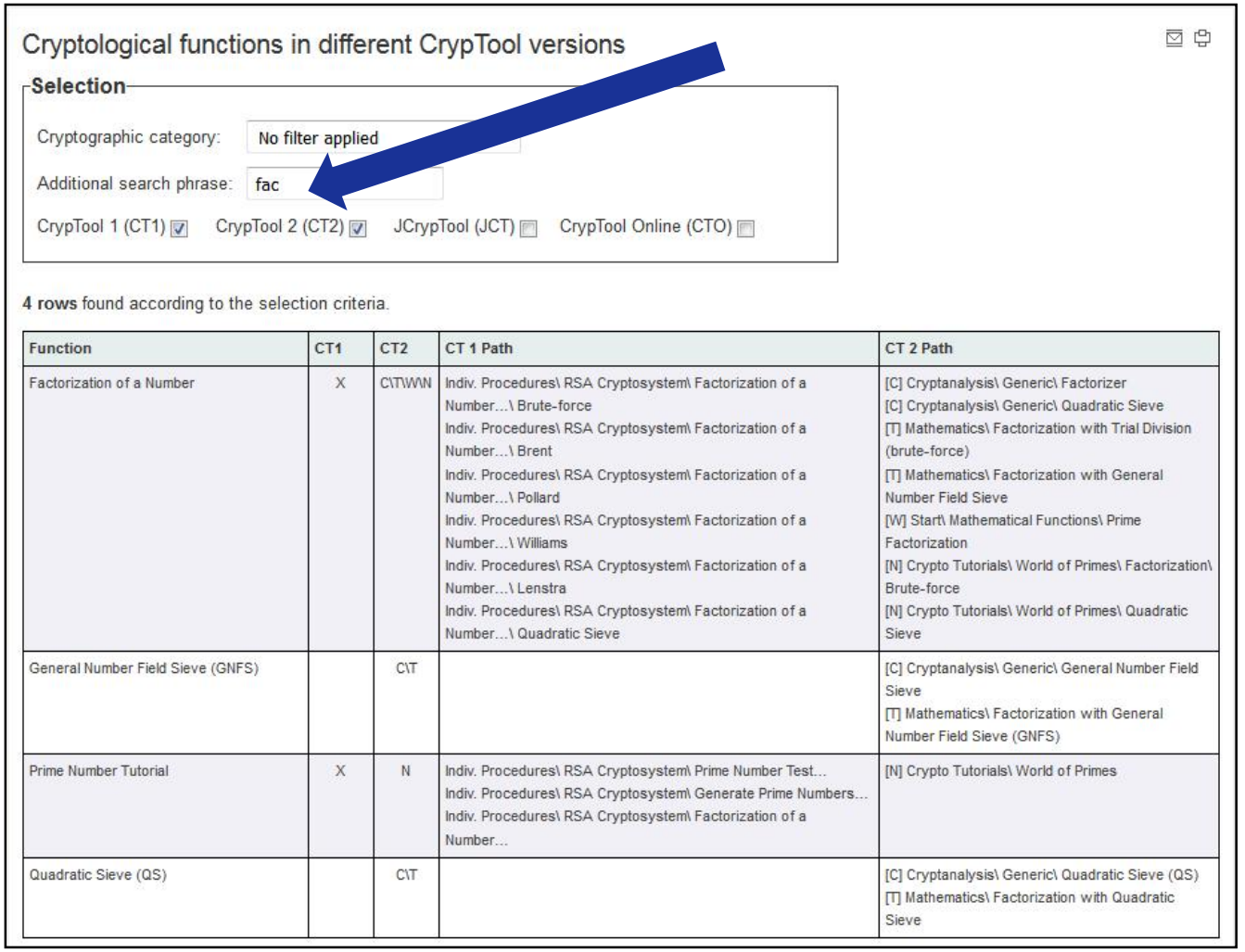
How to Search for Crypto Functionality within CrypTool
http://www.cryptool.org/en/ctp-documentation-en/ctp-functions-en

Within offline programs:

- Online help search
- Filters within CT2 and JCT

On CTP Website:

- Filter on the CrypTool portal from the currently around 260 different functions (from all CT versions)
- http://www.cryptool.org/en/ctp-documentation-en/ctp-functions-en



Cryptological functions in different CrypTool versions

Selection

Cryptographic category: No filter applied

Additional search phrase: fac

CrypTool 1 (CT1) ☑ CrypTool 2 (CT2) ☑ JCrypTool (JCT) ☐ CrypTool Online (CTO) ☐

4 rows found according to the selection criteria.

Function	CT1	CT2	CT 1 Path	CT 2 Path
Factorization of a Number	X	C\T\W\N	Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Brute-force Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Brent Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Pollard Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Williams Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Lenstra Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...\ Quadratic Sieve	[C] Cryptanalysis\ Generic\ Factorizer [C] Cryptanalysis\ Generic\ Quadratic Sieve [T] Mathematics\ Factorization with Trial Division (brute-force) [T] Mathematics\ Factorization with General Number Field Sieve [W] Start\ Mathematical Functions\ Prime Factorization [N] Crypto Tutorials\ World of Primes\ Factorization\ Brute-force [N] Crypto Tutorials\ World of Primes\ Quadratic Sieve
General Number Field Sieve (GNFS)		C\T		[C] Cryptanalysis\ Generic\ General Number Field Sieve [T] Mathematics\ Factorization with General Number Field Sieve (GNFS)
Prime Number Tutorial	X	N	Indiv. Procedures\ RSA Cryptosystem\ Prime Number Test... Indiv. Procedures\ RSA Cryptosystem\ Generate Prime Numbers... Indiv. Procedures\ RSA Cryptosystem\ Factorization of a Number...	[N] Crypto Tutorials\ World of Primes
Quadratic Sieve (QS)		C\T		[C] Cryptanalysis\ Generic\ Quadratic Sieve (QS) [T] Mathematics\ Factorization with Quadratic Sieve

Wishes & Future

- Feedback, criticism, suggestions, and ideas (e.g. include privacy stuff)
- Integration of additional algorithms, protocols, analysis for CT2, JCT and CTO
- Developers, testers, translators, people who commit to take care for a while
- Administrators for the websites (e.g. Joomla upgrade) and the development environments
- Especially a JS developer for CTO
- In particular, university faculties that use CrypTool for educational purposes are invited to contribute to the further development of CrypTool.
- Users who make a significant contribution can request to be referenced by name in the online help, the readme file, the about dialog, and/or on the CrypTool website.

Wishes to you today:

- Offer your students seminar projects and thesis to enhance CT2, JCT and CTO
- Create challenges for MTC3
- Use it yourself in your exercises, your lectures or as research framework
- Spread the word.

esslinger@fb5.uni-siegen.de

Thanks for your attention!